Pk-yrityksen tietoturvan kehittäminen tietoriskianalyysia käyttäen

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittely

Visamäki,

Mika Kalmi

Tietojenkäsittely
Hämeenlinna

Työn nimi	Pk-yrityksen tietoturvan kehittäminen tietoriskianalyysia käyttäen
Tekijä	Mika Kalmi
Ohjaava opettaja	Erkki Laine
Hyväksytty	_____._____.20_____
Hyväksyjä	

HAMK
HÄMEEN AMMATTIKORKEAKOULU

VISAMÄKI
Tietojenkäsittelyn koulutusohjelma
eLearning ja multimedia

Tekijä Mika Kalmi **Vuosi** 2010

Työn nimi Pk-yrityksen tietoturvan kehittäminen tietoriskianalyysia käyttäen

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli tutkia suomalaisten pienten ja keskisuurten yritysten tietoturvan kehittämistä. Tutkimus toteutettiin case-yritykselle, jossa työskentelee kuusikymmentä henkeä. Case-yritystä ei esitellä tarkemmin tutkimuksessa. Tutkimuksen tavoitteena oli selvittää, kuinka pk-yrityksissä voisi kehittää tietoturvaa tietoriskien tunnistamisen ja arvioinnin kautta.

Työn teoriaosuudessa käsitellään tietoturvaa, riskejä, riskien hallintaa ja tietoriskien arviointia. Teoreettisen osan tavoiteena on selvittää tietoturvan määrite, sen osa-alueet, suunnittelu, hallinnointi ja tietoriskien arvioinnin lähestymistavat sekä riskienhallinta osana tietoturvallisuutta.

Tutkimus toteutettiin syksyllä 2010 kvalitatiivisena kyselylomakkeen tukemana haastatteluna. Haastateltavina olivat case-yrityksen johto ja muut avainhenkilöt - yhteensä kymmenen henkilöä.

Tutkimuksen tuloksena voidaan osoittaa, että tietoturvan kehittäminen tulisi huomioida osana liiketoimintaa pk-yrityksissä. Keskitetty, järjestelmällinen ja liiketoimintaan sidottu tietoturvan hallinta parantaa yrityksen tietoturvaa ja tukee samalla liiketoiminnan kannattavuutta, kasvua ja laatutoimintaa. Tukimuksen case-yrityksen toiminnassa ilmeni useita tietoturvan kehityskohteita, joiden keskeisin syy oli keskitetyn tietoturvan kehittämisen ja hallinnan puute. Case-yrityksen suurimmat haasteet tietoturvan kehittämisessä ja hallinnassa olivat organisaation sisäisessä tiedottamisessa ja työtehtävien edellyttämän koulutuksen puutteellisuudessa.

Avainsanat Tietoturva, riskienhallinta, tietoriskit, tietoriskien arviointi.

Sivut 44 s. + liitteet 7 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

VISAMÄKI
Degree Programme in
Business Information Technology

Author Mika Kalmi **Year** 2010

Subject of Bachelor's thesis Information security development with security risk-analysis tool in small and medium-sized enterprise

ABSTRACT

The purpose of this thesis was to develop and apply Information Security in Finnish small and medium sized enterprises. The analysis was made for a case company, with 60 employees. The name of the company remains confidencial in this analysis. The objective of this analysis was to find out how information security should be developed in small and medium sized enterprise, in terms of information risk analyses and risk assessment tools. The theoretical frames of references are processed information security, risks, risk management and approach methods of information security risks. The aim was to analyze information security concepts, districts, management, approach method of information security risks and risks management as parts of information security

The empirical study was conducted in autumn of 2010 as a qualitative inquiry via checklists and interviews. The study was focused on case company management including company key personnel. 10 persons participated in the survey.

Results from the empirical study indicated that developing of Information Security should be assessed as a part of the business in small and medium sized companies. The study demonstrated that centralized managed and organized Information Security management, which is tied up on daily business, is profitable through increased efficiency and as increased level of Information security. The study exposed several Information Security development needs and vulnerabilities in the case company. These development needs and vulnerabilities were mainly caused by lack of centralized management of Information security development and management. Major challenges for the case company were poorly organized internal communication and the management's lack the required knowledge to successfully perform the duties required for their positions.

Keywords Information security, risk management, information security risks.

Pages 44 p + appendices 7 p.

SISÄLLYS

1 JOHDANTO 1

2 TIETOTURVA 2

2.1 Tieto 2
2.2 Tietoturvallisuuden komponenttien määritelmä 3
2.3 Tietoturvallisuuden osa-alueet 5
2.4 Tietoturvallisuuden suunnittelu ja hallinnointi 6
2.5 Kokonaisturvapolitiikan määrittäminen ja turvallisuusjohtamisen alueet 8

3 RISKIENHALLINTA OSANA TIETOTURVAA 10

3.1 Riski 10
3.2 Riskikäsitteet 11
3.3 Riskienarviointi- ja hallintaprosessi 13
3.3.1 Riskientunnistaminen ja arviointi prosessi 13
3.3.2 Riskienhallinta 14

4 TIETORISKIEN ARVIOINTI 17

4.1 Tietoriskien arvioinnin lähestymistapa 17
4.2 Standardit 21

5 PK-YRITYKSEN RISKIENTUNNISTAMINEN 22

5.1 Tietoriskianalyysin toteuttamisen tarpeet 22
5.2 Projektin ja case-tutkimukseni aloitus ja sen tavoitteiden määrittely 23
5.3 Tietoturvariskien arvioinnin lähestymistavan määrittäminen 24
5.4 Sähköisen kyselylomakkeen luominen tarkistuslistasta ja kyselyn toteutus 26

6 AINEISTO JA SEN ANALYSOINTI 29

6.1 Johdon tietoisuus 30
6.2 Toimintaympäristön, työ- ja palvelutilojen turvallisuus 32
6.3 Tietojärjestelmien suojaus 34
6.4 Henkilöstön tietoisuus ja toimintatavat 36
6.5 Liiketoiminnan kehittämistarpeet tietoturvallisuuden toteuttamiseksi 40
6.6 Kyselyn toimivuus 41

7 YHTEENVETO 43

LÄHTEET 45

Liite 1 Tarkistuslistat

1 JOHDANTO

Tässä tutkimuksessa käsittelen pienten ja keskisuurten yritysten (pk-yritykset) tietoturvaa, riskien tunnistamista ja riskienhallintaa tietoturvan riskianalyysin avulla. Pk-yrityksissä tietoturvan toteuttaminen ja hallinnointi on erittäin haasteellinen tehtävä siinä vaadittavan erityisosaamisen ja tarvittavien resurssien puutteen vuoksi. Monissa pk-yrityksissä liiketoiminnan prosesseja ei ole määritelty eksplisiittisesti, vaan niitä hallitaan ja opitaan päivittäisen työn käytännöistä. Liiketoimintaympäristö ilman dokumentoituja liiketoimintaprosesseja luo tietoturvan kehittämiselle haasteita, joita tarkastelen tutkimuksessani. Tietoturvan riskianalyysi käsite tarkoittaa tässä tutkimuksessa riskien tunnistamista ja niiden priorisointia.

Case-yritys, jolle tutkimus toteutettiin, on suomalainen pk-yritys, jolla on liiketoimintaa Euroopassa, Aasiassa ja Pohjois-Amerikassa. Yrityksen palveluksessa on tällä hetkellä noin 60 työntekijää. Liiketoiminta perustuu sisällöntuottamiseen ja jakeluun. Tässä tutkimuksessa tarkastellaan tietoturvaa yrityksen Suomen liiketoiminnan ja toimiston kontekstissa. Yritystä ei mainita tutkimuksessa nimellä, koska yrityksen identifioiminen ei tarjoaisi tutkimukselle lisäarvoa.

Tutkimuksen tavoitteena on selventää hyviä tietoturvakäytäntöjä pk-yrityksen liiketoiminnan tarpeisiin ja löytää sopiva lähestymistapa tietoturvariskien analysointiin. Tässä tutkimuksessa tutkimusongelma voidaan määritellä kahden pääongelman avulla. Pääongelmat voidaan esittää seuraavasti:

- Mitä on tietoturva?
- Miten Pk-yrityksen tietoturvaa voidaan kehittää?

Tutkimuksen teoriaosuudessa tarkastelen seuraavia käsitteitä: tietoturva, riski, riskienhallinta, tietoriskien arviointi - ja erilaiset lähestymistavat tietoriskien arvioinnissa. Tutkimukseni soveltavassa osuudessa toteutetaan case-yrityksen tietoriskien tunnistaminen. Riskianalyysin ainestonkeruu toteutettiin englanniksi, koska case-yrityksen liiketoimintakieli on englanti.

2 TIETOTURVA

2.1 Tieto

Tieto-käsitettä käytetään suomenkielessä vaihtelevasti. Viittaan tutkimuksessani tiedon eri ilmenemismuotoihin seuraavan määritelmän mukaisesti.

Data on muokkaamatonta raakatietoa; esimerkiksi merkkijono. Datalla on oltava yhtenäinen malli (esimerkiksi kieli, tietokanta, numero- tai kirjainjärjestelmä), jolla se muodostetaan ja jonka mukaan sitä voidaan tulkita informaatioksi. Informaatio on mahdollista tietoa. Merkkijonon ilmaiseman viestin sisältö on informaatiota. Informaatio on merkityksellistä jollekin tosiasialle, mutta tietoa se on vasta, kun se merkityksellistyy käyttäjälleen. Tieto on informaatiota, jolla on merkitystä tai välineellistä arvoa tiedon omistajalle tai käyttäjälle. Se on tulkittua, sisäistettyä informaatiota. (Leppänen 2006, 66 – 69.)

Tiedosta on tullut nyky-yhteiskunnassa keskeinen pääoma, tärkein kustannuserä ja ratkaiseva voima (Drucker 1970, 9). Tiedon tai pragmaattisen informaation arvo perustuu siihen, että sen avulla saavutetaan merkittäviä ajan, työn ja rahan säästöjä (Karvonen 2000, 15).

Tieto on aina jonkin tahon omaisuutta ja sille tulisi määritellä juridinen ja hallinnollinen omistaja. Esimerkiksi tieto voi olla vapaasti käytettävissä, mutta sen käyttämiseksi voidaan vaatia täyttämään muotoseikkoja, kuten tekijänoikeuksien mainitseminen lähdetietoina. Tiedolla on aina jokin kohde, joka voi olla monenlaisessa eri formaatissa - esimerkiksi dokumentaatio, laite, ajatus, data tai idea. Tiedonkohde on se, johon tietoturvassa keskitytään. Fyysinen tiedonkohde voidaan suojata fyysisesti, ideat ja osaaminen voidaan suojata sopimuksilla. Ennen tiedon suojaamista suojattava tieto on määriteltävä. Tietoturvallisuustoimenpiteet kehitetään suojattavan tiedon mukaan, jotta voidaan varmentaa tiedon hyödyntäminen yrityksen tarpeisiin. (Leppänen 2006, 66 – 69.)

Yritystoiminnassa tieto on edellytys yrityksen tavoitteiden saavuttamiselle. Tiedon menettäminen voi pahimmillaan johtaa liiketoiminnan keskeytymiseen. Henkilöiden työajalla tai oleellisesti työhön liittyvässä tutkimisessa heidän luomansa uudet innovaatiot ovat yritysten omaisuutta, paitsi jos tiedon omistajuus on erikseen toisin määritelty. Oppilaitoksissa taas opiskelijoiden innovaatiot voivat olla opiskelijoiden omaisuutta. Yritys omistaa toimintaansa liittyvän ja kustantamansa luodun uuden tiedon. Esimerkiksi jos työntekijä kehittää työnsä ohessa työhönsä liittyvän keksinnön, niin työnantajalla on oikeus tähän tietoon. Tiedon omistajuus määritellään yrityksen ja työntekijän työsuhteen ja heidän välistensä sopimusten perusteella. (Leppänen 2006, 66 – 69.)

2.2 Tietoturvallisuuden komponenttien määritelmä

Tietoturva luo pohjan luotettavalle tiedon käsittelylle. Tietoturvan klassinen määritelmä rakentuu kolmen perustekijän varaan luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability), josta käytetään myös usein termiä käytettävyys. (Järvinen 2002, 21–24.) Näitä tietoturvallisuuden perustekijöitä suojataan laitteisto- ja ohjelmistovirheiltä sekä luonnontapahtumien tai tahallisten ja tapaturmaisten inhimillisten toimenpiteiden aiheuttamilta uhkilta ja vahingoilta. (Knuuttila 1997, 111.)

Klassisen määritelmän heikkoutena on, ettei se huomioi tiedon tuottajan tai omistajan identiteettiä, eikä laitteistojen tai tieto- ja tietoliikennejärjestelmien merkitystä tietoturvallisuudessa. Yleisin laajennettu tietoturvallisuuden määritelmä rakentuu seuraavista osatekijöistä: luottamuksellisuus, eheys, saatavuus, kiistämättömyys (non-repudiation) ja pääsynvalvonta (access control). Todentaminen on luottamuksen ja kiistämättömyyden perusedellytys, jonka takia todentaminen ei sisälly erillisenä käsitteenä tietoturvallisuuden laajennettuun määritelmään. Todentaminen tarkoittaa tietojärjestelmien käyttäjien ja laitteiden luotettavaa tunnistusta. Huomionarvoista on, että klassisen määritelmän osat on oltava kunnossa ennen siirtymistä laajennettuihin tietoturvallisuuden osatekijöihin. (Hakala, Vainio & Vuorinen 2006, 5-6.)

Tiedon *luottamuksellisuuden* tarkoituksena on taata, ettei tietoa pääse käyttämään kukaan, kenellä ei ole oikeutta käsitellä määriteltyä tietoa. Tieto on tarkoitettu vain henkilöille, joille on annettu oikeus tietoon. Luottamuksellisuuden edellytys on oikeutetun käyttäjän todentaminen luotettavasti ja tiedon riittävä suojaaminen oikeudettomilta käyttäjiltä. (Järvinen 2002, 22.) Luottamuksellisuuden toteutumiseen pyritään suojaamalla tietojärjestelmien laitteet lukoin ja tietovarastot käyttäjätunnuksin ja salasanoin. Salakirjoitusmenetelmät soveltuvat hyvin tiedon suojaamiseen luottamuksellisuuden kohottamiseksi. (Hakala ym. 2006, 4.) Luottamuksellisten tietojen joutuessa ulkopuolisen tahon haltuun on tiedon hallussapitoa loukattu. Luottamuksellisuuden menettäminen saattaa aiheuttaa yritykselle vakavia taloudellisia sekä imagoon kohdistuvia haittoja. Esimerkiksi tuotekehitystietoja voidaan menettää kilpailijalle, jolloin oma tuote ei kerkiä markkinoille ennen kilpailijan tuotetta. (Miettinen 1999, 25.)

Tiedon e*heyden* tarkoituksena on taata käyttäjille, että tieto on muuttumatonta. Tiedon luvaton muuttaminen on estetty oikeudettomien tahojen toimesta pääsynvalvonnalla. (Järvinen 2002, 22–24.) Eheyden säilyttäminen tarkoittaa tiedon muuttumattomuutta koko tiedon elinkaaren ajan - tietojenkäsittelyn jokaisessa vaiheessa. (Miettinen 1999, 26). Eheys on saavutettu, kun tieto on siinä tilassa kuin sen on alun perin suunniteltu olevan. Eheys voi rikkoutua monella eri tavalla esimerkiksi tietojärjestelmän toimintahäiriön, tietokonevirusten, tietokannan vioittumisen tai tiedonsiirron aikana tehtyjen luvattomien muutosten takia. Tiedon eheyden menettämiseen voivat myös johtaa käyttäjän henkilökohtaiset virheet ja toimet, kuten tiedostojen tahaton poistaminen tai ylikirjoittaminen tai tarkoituksenmu-

kainen dokumenttitietojen väärentäminen. (Miettinen 1999, 25–26.) Eheyden saavuttamiseksi käytetään pääasiassa ohjelmateknisiä ratkaisuja, kuten syöttörajoitteita, syötteen tarkistuksia, tallennus- ja tiedonsiirto-operaatioiden varmistussummia tai tiivisteitä. Tietoliikenneratkaisuisissa etusijalla ovat laitteet, jotka sisältävät virheen tunnistus- ja korjausmenetelmiä. (Hakala ym. 2006, 5.)

Tiedon *saatavuuden* tarkoituksena on taata käyttäjille, että tietojen ja palveluiden tulee olla saatavilla aina, kun tietoa tai palvelua halutaan käyttää. Saatavuuden takaamiseksi järjestelmien tulee olla toimintavarmoja ja varmistettuja. Ulkoisten palveluiden esimerkiksi verkkopalveluiden, tulee olla saatavilla 24 tuntia vuorokaudessa. (Järvinen 2002, 24.) Jos yrityksen tarvitsemia tietoja ei voida käyttää tarvittaessa, saatavuutta ei ole saavutettu (Miettinen 1999, 25–26). Saatavuuden varmistamiseksi tulee huolehtia, että tieto- ja tietoliikennejärjestelmien laitteiden suorituskyky on palveluiden edellyttämällä tasolla. Ohjelmien on myös sovelluttava tallennettujen tietojen käsittelyyn. Saatavuuden parantamiseksi olisi hyvä pyrkiä tuottamaan tietoa saatavuuden toteutumisesta. Raportointitieto mahdollistaa palveluiden kehittämisen tarpeita ja vaatimuksia vastaavaksi. (Hakala ym. 2006, 4-5.) Saatavuutta voi vahingoittaa moni erillinen tekijä. Ulkopuolinen tietoverkkohyökkäys, tekniset häiriöt, sähkökatkokset, laiteviat, laitevarkaus, tekniikan vanheneminen tai verkkoyhteyksien katkeaminen voivat aiheuttaa keskeytyksiä saatavuudessa. (Järvinen 2002, 24.) Saatavuudessa tulee huomioida tiedon hyödyllisyys. Tiedon on oltava sellaisessa muodossa, että sitä voidaan käyttää. Esimerkiksi suojattu tieto, jonka salausavaimet ovat kadonneet, on omistajansa hallussa, mutta ei hyödynnettävissä. (Miettinen 1999, 28.)

Pääsynvalvonta tarkoittaa menetelmiä, joilla hallitaan tietojenkäsittelyinfrastruktuurin käyttöä. Pääsynvalvonta ei käsitä tietoihin pääsyn estämistä. Henkilökunnan halutaan käyttävän yrityksen ohjelmia, laitteita ja tietoverkkoja työasioiden hoitamiseen. Asiaton käyttö tulee estää. Ulkopuolisten ei haluta käyttävän yrityksen laitteita ja verkkoja omiin tarkoituksiinsa. Luvaton käyttö voi aiheuttaa monenlaisia ongelmia, kuten laitteistojen ja tietoliikenneverkkojen kuormittumista, joka näkyy heikentyneenä käytettävyytenä. Luvaton käyttö kasvattaa riskiä haittaohjelmien leviämiselle tietojärjestelmissä, joka johtaa eheys- ja luotettavuusongelmiin. (Kuusela & Ollikainen 2005, 249–250.) Pääsynvalvonnan hallinnointiin tarvitaan määritykset ohjelmistojen, laitteiden, tietoverkkojen ja tietojärjestelmien hyväksyttävästä käytöstä. Määritykset käsittävät ainakin seuraavia kohtia: käyttöajat, etäyhteydet, siirrettävien laitteiden käyttäminen, sallitut laitteet ja niiden käyttöoikeudet. (Hakala ym. 2006, 5–6, 85–86.)

Kiistämättömyyden tehtävänä on tunnistaa ja tallentaa luotettavasti käyttäjän tiedot. Kiistämättömyydellä on kaksi tavoitetta: tiedon alkuperän varmistaminen ja olemassa olevaan tietoon kohdistuvan luvattoman käytön todentaminen. Kiistämättömyyden määritelmät ja vaatimukset saattavat perustua lainsäädäntöön esimerkiksi henkilökunnan oikeusturvan varmentamiseksi. Kiistämättömyyteen pyritään salasanoin, älykortein, sertifikaatein, henkilötodistuksilla, käyttöluvilla ja biometrisellä tunnistamisella. (Hakala ym. 2006, 5, 86.) Kiistämättömyys eli tiedon aitouden todentaminen on tärkeää liiketoiminnan linjausten määrittelyssä, rekrytoinneissa,

yritysostojen yhteydessä ja päivittäisessä päätöksenteossa. Väärennetty tieto voi harhauttaa yrityksen johtoa, ja näin ollen tuottaa erittäin vakavaa vahinkoa liiketoiminnalle. (Miettinen 1999, 27.)

2.3 Tietoturvallisuuden osa-alueet

Tietoturvallisuuden suunnittelun lähtökohtana tulisi olla yrityksen kokonaisturvallisuus, joka jaetaan fyysiseen turvallisuuteen ja tietoturvallisuuteen. Fyysinen turvallisuus käsittää yrityksen henkilöstön, toimitilojen ja omaisuuden suojaamisen esimerkiksi väkivallalta, varkauksilta, tulipaloilta tai muilta onnettomuuksilta. Tietoturvallisuus käsittää yrityksen tietopääoman ja tietojärjestelmien suojaamisen. Yrityksen tietoturvallisuus jaetaan yleensä erikseen käsiteltäviin osa-alueisiin. Osa-alueet jäsennetään yrityksen liiketoiminnan mukaan. Osa-alueiden pohjalta luodaan tietoturvallisuussuunnitelma, jonka laatimisessa käytetään tietoturvallisuuden komponentteja. (Hakala ym. 2006, 12, 14, 18.)

Yleinen tapa on jakaa tietoturvallisuus seuraaviin osa-alueisiin: hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöstö-, tietoaineisto-, ohjelmisto-, laitteisto- ja tietoliikenneturvallisuus. Tietoturvallisuuden osa-alueiden luokittelu voidaan tehdä monella eri tavalla, koska kaikki osa-alueet vaikuttavat toisiinsa ja ne sisältävät osittain päällekkäisiä tekijöitä. (Hakala ym. 2006, 12.) Luokittelun toimivuus on riippuvainen soveltamistilanteesta (Miettinen 1999, 15). Tietohallinto on usein vastuussa tietoturvallisuuden eri osa-alueiden hallinnoimisesta. Ei ole kuitenkaan poissuljettu, että jokin toinen taho hallinnoisi tietoturvallisuuden eri osa-alueita. Esimerkiksi henkilöstöturvallisuutta ja fyysistä turvallisuutta hallitaan usein henkilöstö- ja tietohallinnon yhteistyönä. Tärkeää on muodostaa yrityksen toimintaan sopiva tapa toimia. (Hakala ym. 2006, 11–12.)

Hallinnollinen turvallisuus kokoaa muut tietoturvallisuuden osa-alueet yhdeksi kokonaisuudeksi, ja sitä johdetaan joko omana kokonaisuutena tai jonkin toisen johtamiskokonaisuuden osana. Tarkoitus on ensisijaisesti yhdistää tietoturvallisuuden osa-alueet yhdeksi helposti hallittavaksi kokonaisuudeksi. (Miettinen 1999, 18.) Yksinkertaistettuna hallinnollinen turvallisuus käsittää tietoturvan kehittämisen ja johtamisen. Siihen kuuluu yhteydenpito muihin turvallisuudesta vastaaviin tahoihin yrityksen sisällä sekä ulkopuolella toimiviin viranomaisiin ja yhteystyötahoihin. Keskeisimpiä toimintaprosesseja ovat lainsäädännön ja erilaisten yksityisoikeudellisten sopimusten hallinnointi. (Hakala ym. 2006, 12.)

Fyysinen turvallisuus on itsenäinen yritysturvallisuuden osa-alue. Fyysinen tietoturvallisuus käsittää yrityksen toimitilojen ja niissä olevien laitteiden suojaamisen mahdollisilta fyysisiltä uhkilta, jotka voivat kohdistua fyysisiin laitteisiin tai tallennettuun tietoon. Uhkien toteutuessa yrityksen tietoja voi joutua vääriin käsiin tai ne voidaan menetetään. (Miettinen 1999, 19.) Mahdollisia uhkia ovat esimerkiksi ilkivalta, murrot ja ympäristöuhat. Ympäristöuhkiin kuuluvat vesi-, ja palovahingot sekä sähkö- ja lämmitysjärjestelmien toimintahäiriöt. (Hakala ym. 2006, 12.) Toimitilaturvallisuuden tarkoituksena on varmistaa, että yrityksen toimitiloihin pääsee tarvittaessa ja pääsy on hallittu ja valvottu. (Miettinen 1999, 19.)

Henkilöstöturvallisuus on itsenäinen yritysturvallisuuden osa-alue, mutta se käsittää monia yhtymäkohtia tietoturvallisuuteen. (Miettinen 1999, 18.) Tässä tutkimuksessa henkilöstöturvallisuus-käsitteellä viitataan ensisijaisesti näihin yhtymäkohtiin – ei laajasti henkilöstöturvallisuuteen. Henkilöstöturvallisuuden tavoitteena on minimoida tahattomat ja tahalliset inhimilliset toimintaa häiritsevät tekijät. Se keskittyy myös henkilöistä aiheutuviin ja kohdistuviin riskien hallintaan. (Miettinen 1999, 18.) Henkilöstöturvallisuus käsittää ne toimenpiteet, joilla varmistetaan tietojärjestelmien käyttäjien toimintakyky sekä rajataan käyttäjien oikeuksia yrityksen hallussa olevaan tietoon ja tietojärjestelmiin. Toimenpiteitä ovat esimerkiksi varamiesjärjestelyt, tietojärjestelmien käyttäjien koulutus, tietojärjestelmien vastuiden ja oikeuksien määrittelyt sekä tarvittaessa henkilöiden taustatietojen selventäminen. (Hakala ym. 2006, 11.)

Tietoainestoturvallisuus käsittää ne toimenpiteet, joilla varmistetaan niin digitaalisten tietojen kuin fyysisten dokumenttien säilyttämiseen, varmistamiseen, palauttamiseen ja hävittämiseen liittyvät toimet. *Ohjelmistoturvallisuuteen* kuuluu puolestaan ne toimenpiteet, joilla varmistetaan ohjelmien sopivuus suunniteltuihin käyttötarkoituksiin, keskinäinen yhteensopivuus ja toiminnan luotettavuus ja virheettömyys. (Hakala ym. 2006, 11–12.) Ohjelmistoturvallisuudessa tarkastellaan myös ohjelmien sisäisiä suojausominaisuuksia ja erillisiä tiedonsuojausohjelmia. Yleisiä sisäisiä suojausominaisuuksia ovat ohjelman toiminnasta kertovien lokitietojen keruu, pääsynvalvonta ja salasanojen monimutkaisuuksien ja käyttöaikojen määrittäminen. Tyypillisiä erillisiä suojausohjelmistoja ovat virustorjunta, palomuuri, varmuuskopiointi ja salausohjelmistot, joilla voidaan salata tietoliikennettä tai itse tietoa. (Miettinen 1999, 18–19.) Ohjelmistoversioiden ajantasalla pitäminen ja lisenssien hallinta ovat myös osa ohjelmistoturvallisuutta. (Hakala ym. 2006, 11–12.)

Laitteistoturvallisuus käsittää ne toimenpiteet, joilla varmistetaan työasemien ja tietojärjestelmiin kytkettyjen laitteiden tarkoituksenmukainen mitoitus, toiminnan testaus, huollon järjestäminen sekä varautuminen käyttökatkoksiin, laitteiden kulumiseen ja vanhentumiseen. Myös fyysisten vaaratekijöiden huomioiminen kuuluu laitteistoturvallisuuteen. (Hakala ym. 12 2006.) *Tietoliikenneturvallisuteen* kuuluu puolestaan ne toimenpiteet, joilla varmistetaan yrityksen tietoverkkojen, viestijärjestelmien ja tiedonsiirtoratkaisujen saatavuus ja turvallisuus. (Hakala ym. 2006, 12.) Turvallisuudella tarkoitetaan tietojen suojaamista tiedonsiirtojen aikana niin sisä- kuin ulkoverkossa. Tavoitteena on häiriötön tiedonsiirto, tiedon eheyden ja luottamuksellisuuden säilyttäminen. Nämä tavoitteet tulee huomioida, niin yrityksen sisäverkossa kuin yleisessä verkossakin. (Miettinen 1999, 18–19.)

2.4 Tietoturvallisuuden suunnittelu ja hallinnointi

Tietoturvallisuuden kehittäminen nähdään usein erillisenä tietohallinnon kehittämiskohteena, jolloin tietoturvallisuuden suunnittelu ja kehittäminen vastuutetaan tietohallinnolle. Jos tietohallinto toteuttaa johdon antaman tehtävän ilman muiden tahojen sitouttamista, on yrityksen tietoturvalli-

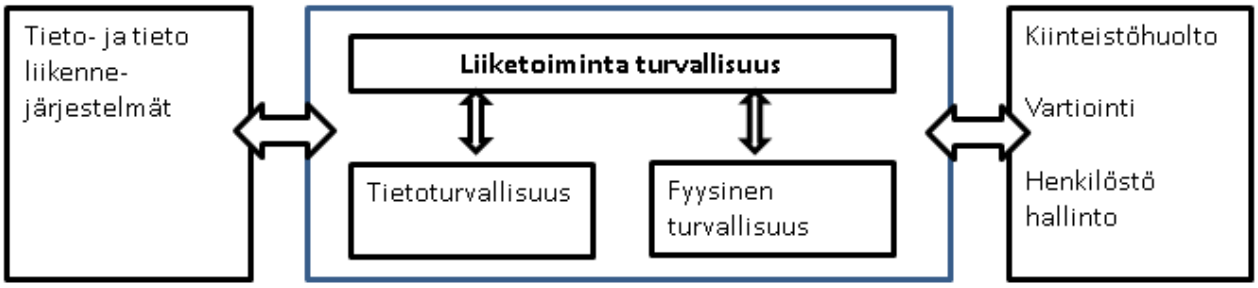
suussuunnitelma toteutettu yksinomaan tietohallinnon näkökulmasta. (Hakala ym. 2006, 14, 18.) Yrityksen tietohallinnolla on harvoin täydellinen kokonaisnäkemys yrityksen liike- ja toimintaprosesseista. Mikäli yrityksen tietoturvallisuutta ei ole suunniteltu riittävän laajasta näkökulmasta, voi organisaatioon syntyä kaksi erillistä turvakulttuuria ja päällekkäisiä työprosesseja hankaloittavia tietoturvajärjestelmiä. Pahimmassa tapauksessa toisistaan suunnitteluvaiheessa tietämättömät ratkaisut saattavat olla ristiriidassa keskenään. (Hakala ym. 2006, 14, 18.)

Tietoturvallisuuden suunnittelu tulisi aina toteuttaa tiimityönä tai projektina, jonka jäsenillä on yhdessä riittävä kokonaisnäkemys yrityksestä ja sen toimintaprosesseista. Huomionarvoista on, etteivät usein edes prosessinomistajina toimivat esimiehet ole riittävän tietoisia prosesseihin liittyvistä yksityiskohdista ja työmenetelmistä. Työntekijöiden ottaminen mukaan suunnitteluprosessiin voi olla hyödyksi paitsi eri näkökulmien huomioimisessa myös tietoturvatietoisuuden leviämisessä yrityksessä. Tietoturvallisuussuunnitelma voi päätyä suosittelemaan suuria muutoksia yrityksen toimintatavoissa, jolloin monipuolisen suunnitteluryhmän osallistuttaminen suunnitteluun vähentää todennäköisesti huomattavasti muutosvastarintaa. Tietoturvallisuuden kehittämiseen tulisi osallistua tietohallinnon lisäksi tahot, joiden vastuulla on tietoturvallisuuteen liittyviä toimintoja esimerkiksi henkilöstöhallinta ja työsuojeluorganisaatio. Tämä takaa, että tietoturvallisuussuunnitelmassa huomioidaan eri toimijat ja tietoturvallisuus käsitellään riittävän laajasta näkökulmasta. (Hakala ym. 2006, 14, 18.)

Tietoturvallisuuden suunnittelu tulee aloittaa tietoturvapolitiikan, tähän liittyvien vastuualueiden määrittämisellä ja resurssoinnilla. Seuraavaksi on tärkeää tunnistaa toimintaa uhkaavat jo tiedostetut ja tiedostamattomat riskit. Riskien tunnistamisen jälkeen määritetään haluttu suojauksen taso ja suojauksen hallinta ja seuranta. (Kajava & Siponen 2002, 2-3.) Kun yrityksessä on määritetty tietoturvapolitiikka ja haluttu suojauksen taso, tulee tietoturvallisuusprosessit dokumentoida ylläpidolle ja käyttäjille. Lisäksi sopimuksiin on tehtävä tarpeelliset kirjaukset tietoturvamäärityksiä noudattaen. Tietoturvamittarit tarvitsee suunnitella ja näiden varaan on kehitettävä raportointijärjestelmä. Tietoturvaan liittyen on myös tehtävä palautumissuunnitelma riskien mahdollista toteutumista varten. Yrityksen tiedot tulee luokitella tiedon luottamuksellisuuden mukaan. On myös huolehdittava loppukäyttäjien tietoturvallisuuskoulutuksesta ja mahdollisista harjoituksista tietoturvaan liittyen. (Kajava & Siponen 2002, 3.)

Haasteena *tietoturvallisuuden hallinnalle* on erilliset toimijat, jotka vastaavat osittain fyysisestä turvallisuudesta ja tietoturvallisuudesta. Yhteistoiminnan kehittäminen on tärkeää. Yrityksen tulisi aina arvioida tilanne, onko tarvetta organisaatiomuutoksille. Usein ei ole tarpeellista luoda esimerkiksi uutta turvallisuusyksikköä tai eriyttää tietoturvallisuutta jollekin tietylle osastolle. Organisatorisesti haluttu lopputulos saavutetaan, kun turvallisuudesta vastaavat toimijat ovat yhteisen johdon alla. Kokonaisturvallisuudesta tulisikin olla vastuullinen ylimpään johtoon kuuluva taho, joka on vastuussa liiketoimintaturvallisuudesta. Liiketoimintaturvallisuuden hallintaan kuuluvat tietoturvallisuus ja fyysinen turvallisuus. Näiden turvallisuustekijöiden hallinnointiin osallistuvat kaikki yksiköt, joiden vas-

tuulla on jokin yrityksen turvallisuusalue (Kuva 1). (Hakala ym. 2006, 14 - 15.)



Kuva 1 Liiketoimintaturvallisuuden johtamismalli (Hakala ym. 2006, 15).

2.5 Kokonaisturvapolitiikan määrittäminen ja turvallisuusjohtamisen alueet

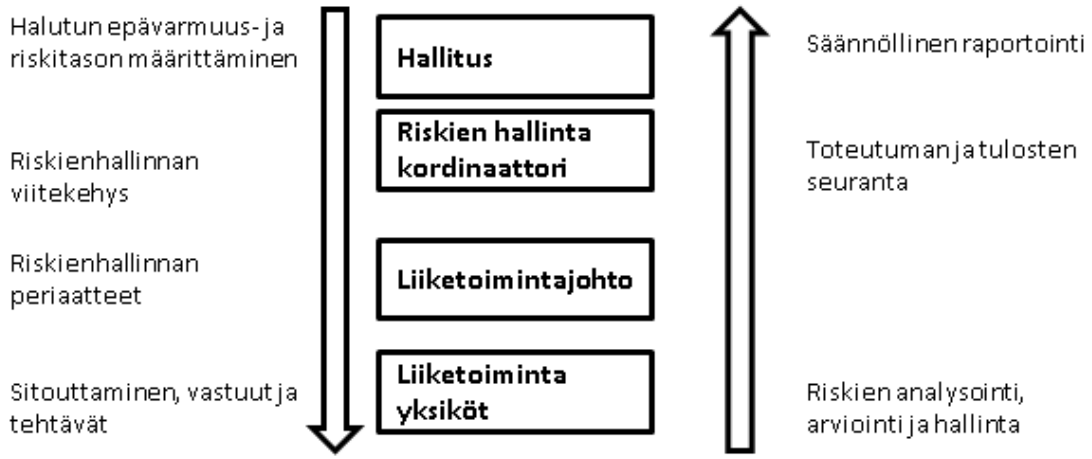
Yritystoiminnan tavoitteena on voittoa tuottava liiketoiminta yrityksen omistajille. Yrityksen strategiaa luodessa toiminnat tulee suunnitella siten, että liiketoiminta on mahdollisimman tuottavaa. Tämän strategian pohjalta muodostetaan turvallisuusjohtamisen strategia. Kokonaisturvapolitiikka on määritettävä, jotta turvallisuusjohtaminen on mahdollista ottaa käyttöön yrityksen liiketoiminnassa. Jo käytössä olevat fyysisen turvallisuuden ja tietoturvallisuuden prosessit käydään läpi ja niistä karsitaan pois ristiriitaisuudet ja päällekkäisyydet. Liiketoimintaprosessien turvallisuustarpeet eritellään. Tavoitteena on löytää eri toimintaprosessien omistajat. Kun prosessit ja vastuussa olevat henkilöt ovat määritelty, voidaan alkaa kehittää yhteistoimintaa. (Leppänen 2006, 21–22.)

Yhteistoiminta ja nykyisten prosessien uudelleen evaluointi voi tuoda huomattavia kustannussäästöjä rinnakkaisten järjestelmien tai prosessien tunnistamisen ja poistamisen myötä. Malliesimerkkinä rinnakkaisista tiedoista ovat henkilötiedot, joita mahdollisesti pidetään yllä useissa järjestelmissä ja useimpien toimijoiden toimesta. Järjestelmiä voivat olla lähiverkot, kulunvalvontajärjestelmät ja sovellus- ja tietokantapalvelimet. Järjestelmät ovat erillisiä, ja tiedon siirto niiden välillä voi olla mahdotonta. Muutokset tehdään useimpiin järjestelmiin manuaalisesti ja tiedot muutoksista tulisi välittää tahoille, jotka ovat vastuussa järjestelmistä. Pahimmassa tapauksessa henkilöiden vaihtaessa työtehtäviä tieto muutoksesta ei välity järjestelmiä ylläpitäville tahoille, jolloin järjestelmissä olevat tiedot vanhentuvat ja lisäävät tietoturvauhkia. Onnistuneessa rinnakkaisuuksien karsinnassa yrityksellä on käytössään yksi henkilöstöhallinnan tietojärjestelmä, josta muut järjestelmät noutavat henkilötiedot. (Hakala ym. 2006, 14–16.)

Perinteisen turvallisuusjohtamisen osa-alueita ovat henkilöstöturvallisuus, työturvallisuus, toimitilaturvallisuus, tietoturvallisuus, ympäristöturvallisuus, palo- ja pelastustoiminta, valmiustoiminta, tuotannon ja toiminnan turvallisuus sekä ulkomaantoimintojen turvallisuus. Uudenaikaiseen turvallisuusjohtamiseen on lisätty liikeriskien ja muiden riskien hallinta. Turvallisuusjohtaminen yhdistää nämä osa-alueet yhdeksi selkeäksi kokonaisuudeksi, eikä keskity painottamaan yhtä näkökulmaa, esimerkiksi tietoturvaa liiaksi. Tällainen toimintamalli tukee turvallisuusjohtamisen tavoit-

tetta eli yrityksen strategian saavuttamista. Turvallisuusjohtaminen on erittäin haasteellista, koska eri osa-alueiden toimintakulttuurit saattavat erota toisistaan jyrkästi. Tämän takia on tärkeä muistaa, että turvallisuusjohtamisen on perustuttava yrityksen strategiaan maksimoida voiton tuottaminen. Silloin keskitytään liiketoiminnan tukemiseen, eikä tietyn osa-alueen liialliseen painottamiseen. (Leppänen 2006, 57–58.)

Eri toimijoilla on erilliset vastuualuensa riskien systemaattisessa hallinnassa (Kuva 2). Yrityksen hallituksen vastuulla on määrittää epävarmuustaso ja päättää, kuinka suuria riskejä liiketoimintajohdon sallitaan ottaa. Epävarmuus luo riskejä ja mahdollisuuksia, joiden avulla voidaan kasvattaa tai pienentää yrityksen arvoa. Johdon valtuuttama riskienhallintakoordinaattori on vastuussa riskienhallinnan viitekehyksen kehittämisestä ja implementoinnista. Riskienhallintakoordinaattori raportoi hallitukselle mahdollisesti kuukausittain. Liiketoiminnan vastuulla on riskienhallinnan strategian ja periaatteiden luonti ja toteutumisen seuranta. Liiketoimintayksiköiden johto on vastuussa liiketoimintayksikkönsä riskienhallintasuunnitelman laatimisesta, seurannasta ja säännöllisestä raportoinnista. (Kuusela & Ollikainen 2005, 126, 130.)



Kuva 2 Johdon rooli riskien hallinnassa (Kuusela & Ollikainen 2005, 131.)

3 RISKIENHALLINTA OSANA TIETOTURVAA

3.1 Riski

Sana riski tarkoittaa asiaa, jonka olemassaolon uskomme tiedostavamme ja johon liittyvästä uhasta tiedämme (Leppänen 2006, 29). Uhka tarkoittaa mahdollista vaaraa, jonka toteutuessa uhan kohteelle tai siihen liittyvälle toiminnalle saattaa aiheutua vahinkoa (Miettinen & Kajava 1994, 4). Ominaista riskille on satunnaisuus, jonka takia on haastavaa ennustaa, milloin tai missä mahdollinen vaara sijaitsee tai toteutuu. Vaaran olemassaolo mahdollistaa kuitenkin uhan riskin toteutumisesta, joka voi aiheuttaa vahinkoa. Riski liittyy aina tulevaisuudessa tapahtuvaan tappion tai vahingon vaaraan. Riski koskeekin tapahtuman seurauksia, ei itse tapahtumaa. Riskin arvioinnissa huomioidaan uhan todennäköisyys ja suuruus eli haitallisuus. Jotta uhan suuruus voidaan määrittää, on arvioitava riskin arvo uhan toteutuessa. (Leppänen 2006, 29–30.)

Päätöksentekoon liittyy aina riskejä, jotka vaarantavat tavoitteen saavuttamisen tai aikaansaavat lopputuloksen, joka poikkeaa odotetusta. Liiketoiminnalle riskinotto on kuitenkin välttämätöntä kilpailukyvyn säilyttämiseksi. (Kuusela & Ollikainen 2005, 15, 28.) Riski on suunniteltavissa etukäteen, jolloin puhutaan riskinotto- tai riskinkantokyvystä - kyvystä toiminnan jatkamiseen normaalisti riskin tapahtuessa (Erola & Louto 2000, 23). Tietoriskillä tarkoitetaan riskityyppiä, joka kohdistuu tietoihin tai tietojen käyttöön liittyvään tapahtumaan, joka toteutuessaan aiheuttaa vahinkoa (Miettinen & Kajava 1994, 4).

Epävarmuus on oleellinen piirre riskeissä, joka sopii huonosti rationaaliseen tietoon perustuvaan riskien hallintaan. Frank Knightin (1885–1972) mukaan epävarmuus on tekijä, joka ei ole mitattavissa ja jonka todennäköisyyttä ei voida laskea todennäköisyyteen ja täydelliseen tietoon perustuen. John M. Keynesin (1883–1946) mukaan todennäköisyysteoria on epäluotettava tosielämän tilanteissa, koska päätöksiä tehtäessä ihmiset muuttavat maailmaa. John V. Neumanin (1903–1957) peliteorian mukaan muiden ihmisten aikomukset ovat todellinen epävarmuuden aiheuttaja, koska pelaajat ennakoivat toisten pelaajien siirtoja. (Kuusela & Ollikainen 2005, 25–29.)

3.2 Riskikäsitteet

Riskit voidaan luokitella dynaamisiin ja staattisiin riskeihin. *Dynaamiset riskit* vaihtelevat suhdanteiden ja olosuhteiden myötä. Dynaamisista riskeistä voi seurata voittoa tai tappiota. Lisäksi toimija voi itse vaikuttaa riskiin ja riskinoton suuruuteen. Dynaamisia riskejä ei yleensä voida siirtää muiden kannettavaksi. Dynaaminen riski voi olla esimerkiksi liiketoiminnan laajentaminen, jolloin yritys ottaa tietoisen riskin tavoitellessaan voittoa. *Staattiset riskit* ovat yrityksen tai yksilön tahdosta riippumattomia ja niiden toteutumisesta ei voi seurata voittoa. Staattisia riskejä toteutuu aina ja niiden todennäköisyyksien ja seuraamusten arviointi on helpompaa kuin dynaamisten riskien. Tämän takia staattiset riskit ovatkin usein siirrettäviä eli vakuutettavia riskejä. Staattinen riski voi olla esimerkiksi tulipalo tai yrityksen omaisuuteen kohdistuva varkaus. (Kuusela & Ollikainen 2005, 33–35.)

Miettinen (1999, 50–53) tarkastelee tietoturvallisuutta kolmen riskikäsitteen kautta: riskien hallinta, riskien arviointi ja riskianalyysi (taulukko 1). Nämä käsitteet tarjoavat työkalut, joilla voidaan tunnistaa liiketoiminnan uhkatekijät tehokkaasti, tarkasti ja nopeasti. Riskit arvioidaan uhan, epävarmuuden ja uhan toteutumisen mahdollisuuden avulla. Uhista arvioidaan seurausvaikutukset päivittäiseen toimintaan. Yritykset keskittyvät tavallisesti tarkastelemaan toiminnalle aiheutuvia uhkia. Epävarmuus liittyy riskiin, joten yrityksen on selvitettävä riski-vaihteluväli sen todennäköisyyden arvioimiseksi. Riskien kääntäminen mahdollisuuksiksi jää yleensä taka-alalle. Riskien tiedostamisen avulla yritys voi kuitenkin löytää merkittäviä kehitysmahdollisuuksia.

Taulukko 1 Riskikäsitteet ja niiden suhteet (Miettinen 1999, 53)

Arvioitava ominaisuus	**Käsitteet**		
	Riskienhallinta	**Riskien arviointi**	**Riskianalyysi**
Käsitteen esitys	Yritykseen kohdistuvien uhkien ominaislaadun ja laajuuden sisäistäminen.	Yritykseen kohdistuvien uhkien toteutumisesta seuraavien vaikutusten arviointi	Yritykseen kohdistuvien uhkien tunnistaminen perinpohjaisen tutkintaprosessin kautta
Yhteys toimintaprosesseihin	Yrityksen johdon prosessi	Arvioidaan tapahtuman toteutuman seuraamusvaikutuksia yrityksen liiketoiminta prosesseihin	Tutkinta prosessi
Kenelle raportoidaan	Ylimmälle johdolle	Ylimmälle johdolle	Ylimmälle johdolle
Käsitteen perustehtävät	Johdon hyväksymän tietoisen riskitason määrittely	Ei-toivottujen tapahtumien priorisointi	Heikkouksien ja riskien etsiminen riskianalyysin kohteesta
	Halutun riskitason saavuttaminen	Toteutuneen ei-toivotun tapahtuman vaikutusten arviointi	
	Yritykseen kohdistuvien riskien systemaattinen seuranta		

Taulukossa 1 on kuvattu riskikäsitteet, jotka jakautuvat riskienhallintaan ja riskien arvioimiseen sekä riskianalyysiin. *Riskienhallinnan* tavoitteena on riskien luonteen ja laajuuden ymmärtäminen, hyväksyttävän riskitason määrittäminen ja olemassa olevan riskitason alentaminen hyväksyttävälle tasolle. *Riskien arviointi* puolestaan käsittää toimenpiteet, joiden avulla yritys pyrkii arvioimaan löydetyt ja havaitut ei-toivotulla tavalla vaikuttavien tapahtumien seuraukset. Siihen kuuluu seurausvaikutusten arviointi ja johdolle raportointi, jos jokin ei-toivottu tapahtuma toteutuu. *Riskianalyysi* on tutkintaprosessi – metodi, jonka päämääränä on etsiä ja löytää systemaattisesti tutkinnan kohteeseen kohdistuvat ei-toivotut tapahtumat (Miettinen & Kajava 1994, 4). Riskianalyysi on teknisempi käsite kuin riskienhallinta tai riskien arviointi ja siihen kuuluu tyypillisesti useita yksityiskohtaisia työvaiheita. (Miettinen 1999, 50-51.)

3.3 Riskienarviointi- ja hallintaprosessi

3.3.1 Riskientunnistaminen ja arviointi prosessi

Riskienhallinnan mahdollistamiseksi on yritykseen kohdistuvat riskit eli uhat tunnistettava ensin ja tehtävä päätös riskienhallinnan aloittamisesta. Tämä tarvitsee ylimmän johdon ehdottoman tuen. Riskien tunnistaminen on toteutettava muodostamalla kokonaisvaltainen kuva toimintaympäristöstä pyrkimättä analysoimaan liian perinpohjaisesti mahdollisia riskejä. Tarkoituksena on hahmottaa organisaation toimintaan liittyvä riskikokonaisuus. (Leppänen 2006, 120–123.)

Riskien tunnistamisessa tulee huomioida myös mahdollisuudet. Jos yrityksellä on toimiva riskienhallinta, niin se voi saavuttaa kilpailuetua toipumalla nopeammin toteutuneista riskeistä ja mahdollistamalla uusien riskien ottamisen. Kilpailija voi myös joutua varomaan uusien riskien ottamista, mikä antaa enemmän tilaa ja mahdollisuuksia markkinoilla yritykselle, joka on tietoinen riskeistään. (Leppänen 2006, 120–123.) Riskien tunnistamisen yhteydessä voidaan tarvittaessa suorittaa karkea arviointi riskien vaikutuksista ja todennäköisyyksistä. Tarkemmassa määrittelyssä voidaan käyttää apuna asiantuntijoita, tilastoja ja herkkyysanalyyseja. (Kuusela & Ollikainen 2005, 138–139.)

Optimitilanteessa riskientunnistaminen voidaan tehdä organisaation tietojärjestelmien dokumentaatioihin perustuen. Kartoitukseen kannattaa käyttää tilanteeseen sopivaa tietoriskien arviointi lähestymistapaa dokumentoinnin ollessa rajallinen tai epätarkka. Riskikartoituksen tulisi käsitellä sekä nykytilannetta että tulevaisuuden uhkia. Jo tiedossa olevat ongelmat ja realisoituneet riskit on järkevä ottaa tällöin lähtökohdaksi, koska järjestelmän käyttäjät muistavat nämä yleensä hyvin. (Hakala ym. 2006, 80–82.)

Tunnistamisen jälkeen seuraa *arviointivaihe*, jossa suoritetaan riskin todennäköisen rahamääräisen vaikutuksen arviointi (Leppänen 2006, 123). Riskeistä arvioidaan, mitä vaikutuksia riskillä on realisoituessaan ja kuinka todennäköinen riski on, kun erilaiset uhkatekijät ja haavoittuvuudet on otettu huomioon. Arviointi perustuu yrityksen määrittämiin riskikriteereihin. Lopputuloksena tulisi olla helposti ymmärrettävä käsitys riskitasosta, jonka perusteella päätetään riskienhallinnan toimenpiteistä. (Hakala ym. 2006, 108.) Riskien arviointiprosessin perusteella luodaan perusta riskienhallinnalle ja mahdolliselle turvallisuusjohtamiselle. Huomionarvoista arvioinnissa on organisaatioon vaikuttavien todennäköisten riskien seuranta. Tämä antaa perusteet riskienhallintatoimenpiteille. Arviointijärjestelmä on oltava koko organisaatiolle ja sen on oltava yhdenmukainen. (Leppänen 2006, 123–124.)

Tietoriskien arviointiprosessi on hyvin samankaltainen kuin muidenkin riskien arviointiprosessi. Hyväksi havaitut menetelmät muiden riskien arvioinnissa toimivat todennäköisesti tietoriskienkin arvioinnissa. Perinteiset riskienarvioinnin ja riskianalyysin mallit eivät sovellu kuitenkaan monimutkaisiin tietoverkkoihin ja tietojärjestelmiin. Ongelman aiheuttaa tiedon abstrakti olemus. Kuinka arvioida kohdetta, jolla ei ole fyysistä olemusta? Tiedolla on erilaisia olomuotoja, kuten sähköinen, magneettinen tai paperi. Tiedon sisällöllä ei kuitenkaan itsessään ole fyysistä olomuotoa. Tämän vuoksi tietoriskien arvioinnissa on keskityttävä fyysiseen esitysmuotoon ja itse asiasisältöön kohdistuviin uhkiin. (Miettinen & Kajava 1995, 10.)

3.3.2 Riskienhallinta

Riskienhallinnan tavoitteena on hallita tunnistettuja riskejä kokonaisvaltaisesti. Riskejä on kaikkialla ja uusi toiminta synnyttää aina uusia riskejä. On mahdotonta hallita kaikkia riskejä ja tähän ei tule pyrkiäkään. Kaikkien riskien tunnistaminen, analysointi ja hallitseminen kuluttaisivat liikaa organisaation resursseja. Riskienhallinnassa on tiedettävä kriittisimmät riskit ja pidettävä riskienhallintatoimenpiteet riittävinä. Riskienhallinnassa on aina huomioitava +1-sääntö eli on varauduttava myös siihen, mitä ei tiedetä. Riskienhallinta perustuu seuraavaan kolmeen seikkaan: riskien tunnistamiseen, mahdollisimman luotettavasti arvioitujen uhkien todennäköisyyden pienentämiseen ja riskien seurausten minimointiin. (Leppänen 2006, 119.)

Riskienhallintaa voidaan käsitellä myös poikkeaman hallinnaksi. Organisaation johto luo vision, jonka toteuttamiseksi rakennetaan strategia. Strategian toteutuessa johdon luoma visio toteutuu. Nyt voidaan nähdä matka lähtötilanteesta vision toteutumiseen täysin strategian mukaisena, eikä se sisällä poikkeamia, jotka estäisivät vision toteutumisen. Poikkeama on riski, joka haittaa strategian toteutumista ja vie organisaatiota kauemmaksi vision toteutumisesta. Hallituissa riskeissä on huomioitava aina jäännösriski. (Leppänen 2006, 120 -121.)

Riskienhallinta on aina suhteutettava toiminnan kannattavuuteen. Riskienhallinnan lähtökohtana on riskien määritteleminen, mitä riskit ovat, mitkä ovat mahdolliset kulut toteutuneesta riskistä ja millä todennäköisyydellä riski toteutuu. Riskienhallinnan kustannuksia on verrattava niihin kustannuksiin, jotka riski toteutuessaan aiheuttaa. (Leppänen 2006, 164.) Omistajat määrittävät yrityksen johdon avulla, millä tasolla ja laajuudella yritys keskittyy riskienhallintaan. Omistajat määrittelevät resurssit ja johto panee käytäntöön omistajien linjaukset (Miettinen 1999, 54–56).

Optimitasolla kulut riskien toteutumisesta ja riskienhallinnasta ovat yhtä suuret. Riskienhallinnan kustannukset eivät saa ylittää riskien toteutumisesta aiheutuvia kuluja, koska tällöin riskienhallinta on kannattamatonta. Riskienhallintakeinoja luodessa on ensin päätettävä, kuka on henkilökohtaisesti vastuussa kuhunkin riskiin liittyvistä toimenpiteistä. Usein riskistä vastaa henkilö, joka on vastuussa prosessista tai prosessin osasta, jota riski koskee. Riskin koskettaessa laajempaa kokonaisuutta on järkevää käsitellä riskiä erillisenä prosessina, jossa on mukana useampia henkilöitä. Tällöin

on määriteltävä henkilöiden vastuiden rajat selkeästi. (Leppänen 2006, 164–165.)

Riskien raportointiin on myös määriteltävä henkilöt, jotka raportoivat riskeistä. Raportointi voidaan toteuttaa poikkeamatarkastelun avulla, jolloin raportoidaan vain asiat, jotka poikkeavat sovituista raja-arvoista. Tällaisessa toimintamallissa riskimittariston suunnitteluun tulee panostaa riittävästi. Tämä mahdollistaa riittävän realistisen kuvan organisaatiolle riskeistä ja niiden hallintakeinoista. Riskiraportoinnissa ajoituksen määrittäminen on tärkeää. Tiettyjä riskejä voidaan ehkä seurata vuosittain, mutta esimerkiksi tapaturmia, läheltä piti -tilanteita ja vaikkapa kassavirtaa koskevia riskejä voidaan seurata päivittäin. (Leppänen 2006, 164–165.)

Vaikka riskit olisivat hallittuja, tulee aina varautua uhan toteutumisen varalle. Varautumissuunnitelma tulisi aina tehdä suunnitteluprosessin aikana. Varautussuunnitelmasta ja vastuualueista tulee tiedottaa koko yrityksessä. Laitteet ja muiden oleellisten asioiden tulee myös olla kunnossa ja niiden käyttö on harjoiteltu ja testattu etukäteen. Näiden toimenpiteiden tukena tulee olla ajan tasalla oleva dokumentointi, jotta johto on kykeneväinen seuraamaan tilannetta. Hyvänä esimerkkinä toimii tulipalo, jota varten on vakuutus, mutta myös jatkuva harjoittelu henkilökunnalle ja valmiiksi hankittu palokalusto uhan toteutumisen varalta. (Erola & Louto 2000, 83–84.)

Riskien hallinnan yleisimmät toteutustavat ovat riskin poistaminen, pienentäminen, siirto ja hyväksyminen. Riski voidaan pyrkiä *poistamaan* kokonaan, jonka jälkeen riski ei ole enää uhka. Riskien poistaminen on yleensä epärealistinen tavoite, vaikka riski voitaisiinkin poistaa, työmäärä ja kustannukset riskin poistamiseksi saattavat tulla kalliimmiksi, kuin itse riski toteutuessaan. (Miettinen 1999, 56.)

Riskien *minimointi* on yleisin riskien hallintatapa. Tämä koskee erityisesti tietoturvariskejä. Huomattava osa nykyisistä suojausmenetelmistä ei poista riskiä, mutta minimoi huomattavasti riskin toteutumisen mahdollisuutta. Esimerkiksi yrityksen lähiverkon suojaaminen palomuurilla, pienentää uhan toteutumista mutta ei poista riskiä. Luvaton tunkeutuminen on edelleenkin mahdollinen riski, mutta luvattoman tunkeutumisen suorittaminen on erittäin haastavaa ilman käyttöoikeuksia. (Miettinen 1999, 56–57.)

Tehokkaita tapoja minimoida riskejä ovat vahingon rajaaminen vain johonkin osaan toimintaa varautumalla laiterikkoihin standardisoidulla ympäristöllä ja luomalla prosessiyhdistelmiä, jolloin osa ellei koko kapasiteettia voidaan laiterikon sattuessa siirtää toimimaan toisille alustoille. Noudattamalla tätä toimintamallia voidaan löytää käytännöllisempiä ja tuloksellisempia toimintatapoja kuin alkuperäinen prosessi. Riskien toteutumista ennakoivien mittaristojen seuranta, reagointinopeuden nostaminen sekä automatisoitujen ja hyvin ohjeistettujen prosessien luominen ovat myös tehokkaita tapoja riskien minimointiin. Oleellista on aloittaa suunnitelmallinen ja hallittu toiminta, jolloin ei tarvitse improvisoida riskin toteutuessa. Liiketoiminnan kannalta sopimukset alihankkijoiden ja asiakkaiden kanssa ovat tärkeässä roolissa. Sopimuksissa voidaan määritellä

ennakkopäätöksiä uhkien toteutuessa esimerkiksi force majeure-ehto. (Erola & Louto 2000, 81–85.)

Riskin *siirto* on kyseessä, kun yritys siirtää tietoisesti riskin jollekin toiselle osapuolelle. Yleensä kyseessä on vakuuttaminen. (Miettinen 1999, 57.) Vakuuttamista ei tule pitää kokonaisvaltaisena riskinhallinta keinona, koska vakuutus ei tyypillisesti kata tapahtuneita vahinkoja kokonaisuudessaan. On epätodennäköistä, että vakuutus korvaisi menetetyn markkina-aseman tai yrityskuvan vahingoittumisen. (Erola & Louto 2000, 80.) Tyypillisimpiä siirrettäviä riskejä ovat palo-, ilkivalta- ja varkausvakuutukset, joilla suojataan yrityksen toimitilat ja kiinteä omaisuus. Yhdistävä tekijä edellä mainituille riskeille on, että niitä ei tavallisesti voida poistaa kokonaan, mutta toteutuessaan riskit voivat pysäyttää, jopa lopettaa yrityksen liiketoiminnan. Tällaisille riskeille siirtäminen on järkevin vaihtoehto. Kaikkia riskejä ei voida siirtää. (Miettinen 1999, 57.) Riskin siirtäminen osittain on järkevää esimerkiksi aloittaessa liiketoimintaa uudessa maassa, voidaan maariskiä vähentää ulkoistamalla toimintoja, joihin riski on sidonnainen. Yleinen tapa on järjestää liiketoiminta maassa paikallisen edustajan kanssa, oman toimiston avaamisen sijasta. (Erola & Louto 2000, 81.) Riskin siirtämisessä on varmistettava, että osapuoli, jolle riski siirretään, on kykenevä käsittelemään riskin asianmukaisella tavalla (Hakala ym. 2006, 108). Esimerkiksi vaarallisten kemikalioiden käsittely on todennäköisesti pakollista ulkoistaa asiantuntijayritykselle (Erola & Louto 2000, 81).

Riskin *hyväksyminen* on kyseessä, kun yritys hyväksyy tietoisesti riskin. Yleensä kyseessä ovat riskit, joiden uhka tai todennäköisyys on pieni tai vähän merkitsevä tai riskille ei voida tehdä mitään. Tyypillinen hyväksyttävä riski on, kun yritys aloittaa liiketoiminnan vieraassa maassa, jonka poliittinen tilanne on epävakaa. Tällöin voidaan harjoittaa liiketoimintaa, mutta yritys ei voi vaikuttaa maan tilanteeseen. (Miettinen 1999, 57.)

Kun riskienhallinta tavasta on päätetty, tulee huomioda vielä olemassa oleva mahdollisuus riskin toteutumisesta eli jäännösriski (residual risk). Jäännösriski ei saa olla suurempi kuin hyväksyttävä riski ja jäännösriskiä varten on oltava toipumissuunnitelma (disaster recovery plan). Riski, jonka toteutumiseen ei ole varauduttu, aiheuttaa todennäköisesti suuremman vahingon, kuin riski jonka toteutumisen varalle on toipumissuunnitelma. (Hakala ym. 2006, 92,98.)

4 TIETORISKIEN ARVIOINTI

4.1 Tietoriskien arvioinnin lähestymistapa

Tietoriskien arviointiin on perinteisesti käytetty sekä kvalitatiivisia että kvantitatiivisia lähestymistapoja. Kvalitatiivisessa tietoriskien arvioinnissa arvioinnit tehdään diskreettejä (epäjatkuvia) muuttujia käyttäen. Arviointi on yleensä sanallista ja tilanteen kuvaamiseksi voidaan käyttää seuraavanlaista asteikkoa: ”tapahtuu kerran päivässä, kuukaudessa tai vuodessa Kvantitatiivisessa tietoriskien arvioinnissa käytetään tarkkoja numeerisia arvoja. Laskutoimenpiteet perustuvat tilastomatematiikkaan tai todennäköisyyslaskentaan. Arvioinnissa voidaan käyttää prosentteja tai lukuarvoja. (Miettinen & Kajava 1994, 13.) Monet organisaatiot käyttävät kvantitatiivisia lähestymistapoja riskien arviointiin. Esimerkiksi vakuutusyhtiöt syöttävät tilastoihin perustuvia lukuja järjestelmään, joka tuottaa riskin toteutumisen todennäköisyyden prosentteina ja mahdollisen vahingon laajuuden rahassa mitattuna. (Kajava & Siponen 2002, 4.)

Tarkkoihin lukuihin luottaminen ei välttämättä ole mahdollista niinkin kapealla ja erikoistuneella alalla kuin tietoriskienhallinta, koska jokainen ympäristö on ainutlaatuinen. Voimme luottaa itse metodeihin, mutta emme tuloksiin, kun vertaamme tuloksia eri tai jopa samoissa organisaatioissa erilaisissa tilanteissa. Tietoriskienhallinta on niin herkkä alue, että yksinkertaisesti tarkkoihin tuloksiin ei voida absoluuttisesti luottaa. Monesti ihmisen kokemus ja herkkyys ovat tehokkaampi tapa arvioida riskien toteutumista. (Kajava & Siponen 2002, 4.)

Tietoriskien arvioinnin tavoitteena on lisätä päätöksentekijän eli yleensä johdon tietämystä tietoriskejä kohtaan ja luoda pohja mm. tietoturvapolitiikalle oikeille päätöksille. Jotta riskienarviota voitaisiin käyttää tehokkaasti, on arvioinnille määriteltävä selkeät ja konkreettiset tavoitteet. Ilman määrityksiä lopputulos on todennäköisesti pinnallinen tai jopa harhaanjohtava. Tällöin todelliset ongelmat eivät tule esille ja syyllistytään helposti virhearviointeihin. (Miettinen & Kajava 1994, 10–11.)

Tietoriskien arviointia varten on lukuisia eri lähestymistapoja. Eräitä käytetyimpiä lähestymistapoja ovat tarkistuslistat, skenaarioanalyysi, haavoittuvuusanalyysi, miellekarttatekniikka, Baseline-menetelmä ja potentiaalisten ongelmien analyysi (POA). Tietoriskien arviointia tehdessä oleellista on, soveltuuko valittu lähestymistapa arvioinnin suorittamiseen vai ei (Miettinen & Kajava 1994, 23).

Tarkistuslistat ovat todennäköisesti yksinkertaisin tapa toteuttaa tietoriskien arviointi. Tarkistuslistoja on valmiina eri toimialoille, joita voidaan käyttää erityisalojen tietoriskien arvioinneissa. (Miettinen & Kajava 1994, 17–18.) Pk-yrityksille on laatinut esimerkiksi PK-RH valmiita kysymyslistoja (http://www.pk-rh.fi/). Yksinkertaisuus ja valmiit pohjat takaavat, että tarkistuslistat ovat halpa ja nopea tapa toteuttaa tietoriskien arviointi. Tar-

kistuslistojen käyttö ei myöskään edellytetä, niin syvällistä osaamista kuin muut lähestymistavat. (Miettinen & Kajava 1994, 17–18.) Tarkistuslistat sisältävät tietyn riskikartan riskit, kuten tietoriskit. Tarkistuslistat on yleensä sovitettu tietyille toimialoille tai tietyntyyppisiin riskeihin. Tarkistuslistojen heikkoutena on kuitenkin kysymysten yleisluonteisuus. Tarkistuslistat tulisi aina sovittaa organisaation toiminnan mukaisiksi ja niiden tulee käsittää selviteltävät asiat. Tarkistuslistoihin tulisi pyrkiä sisällyttämään mahdollisimman paljon toimivia käytäntöjä. Näin tarkistuslistat toimivat myös turvallisuusohjeena ja samalla helpottavat toiminnan tavoitetason määrittämistä. (Leppänen 2006, 133.)

Tehokkaimpia tarkistuslistat ovat virheiden, olemassa olevien ja puuttuvien suojausten tarkistamiseen. Uhkien etsinnässä tarkistuslistat eivät ole toimivia ja ne eivät sovellu suojauksien toimivuuden ja käytännöllisyyden arviointiin yksittäisiä tietoturvauhkia vastaan, koska lopputuloksena on usein suurpiirteinen kuvaus kohteen nykyisestä tilasta ja tarvittavista kehitystoimenpiteistä. (Miettinen & Kajava 1994, 18.) Tarkistuslistassa on kuvattu riski ja riskin tila yrityksessä. Listoihin voidaan merkitä, mikä on riskin tila yrityksessä, esimerkiksi riski on hallinnassa tai ei ole hallinnassa. Listoihin on myös hyvä jättää tilaa muistiinpanoille ja mahdollisille esimerkeille, jos riski toteutuu. (Leppänen 2006, 134.)

Skenaarioanalyysi on erittäin suosittu menetelmä tietoturvariskien kartoittamiseksi. Perusideana on mahdollisten uhkatekijöiden tunnistaminen, jotta uhkatekijöihin voitaisiin valmistautua. Yleensä skenaarioanalyysi muodostuu pienistä kertomuksista eli skenaarioista, joilla mallinnetaan oletettuja uhkatilanteita. Skenaarioissa kuvataan eri uhkatilanteita ja mahdollisia seuraamuksia kohteelle tai siihen liittyvälle prosessille uhkien realisoituessa. (Miettinen & Kajava 1994, 18.)

Skenaarioanalyysi aloitetaan skenaarioiden luomisella, minkä jälkeen skenaariot annetaan organisaation johdolle arvioitavaksi. Johto tekee tarvittavat muutosehdotukset skenaarioihin. Prosessia jatketaan kunnes skenaariot on tavoitettu ja koostettu yhteen. Skenaarioiden tulee sisältää nykyiset suojaukset, esittää tietoturvan parannusehdotukset sekä kuvata havaitut puutteet. Skenaarioiden muodostamisen vahvimpia puolia on kommunikoinnin ja näin yhteisen ymmärryksen lisääminen eri osapuolien välillä. (Miettinen & Kajava 1994, 18.)

Haavoittuvuusanalyysi on tunnetuimpia riskianalyysimenetelmiä ja toimii samalla periaatteella kuin kysymyslistat. Lähtökohtana on tarkastella koko organisaation toimintaa yleisellä tasolla. Organisaation toiminta voidaan jakaa esimerkiksi seuraaviin osa-alueisiin (Leppänen 2006, 134–135.):

- henkilöstö
- talous, rahoitus, johtaminen
- tuotanto, tuotteet
- alihankinta, ostot, kuljetukset, varastointi
- myynti, markkinointi, asiakkaat
- kilpailijat, suhdanteet
- investoinnit
- normit, julkinen valta, sidosryhmät

Tarkastelu etenee yhdestä aihekokonaisuudesta pienempiin kokonaisuuksiin uusien haavoittuvuushavaintojen ilmetessä. Haavoittuvuusanalyysin tuloksena on karkea kokonaiskuva organisaatiosta tai sen tiettyjen osien haavoittuvuudesta. Haavoittuvuusanalyysiin kirjataan riskin pääotsikko ja vahinkoesimerkki, merkitään riskin nykyinen tila (ei riskiä – riski hallinnassa – hoidettava kuntoon – ei koske meitä) karkealla arvioinnilla (3·3 menetelmä) sekä kirjataan kehittämistoimenpiteiden suunnittelu, toteutus ja seuranta. Arvioinnin yhteydessä on hyvä tehdä tarkentavia kuvauksia riskistä ja siihen liittyvistä muuttujista. Haavoittuvuusanalyysissa merkittävintä on riskien esiin tuominen, mikä käynnistää riskeistä keskustelemisen ja tuo esiin eri näkökulmia. Tämä johtaa parhaillaan työskentely ja toimintatapojen uudelleen evaluointiin. (Leppänen 2006, 134–135.)

Miellekarttatekniikan tavoitteena on purkaa hiljaista tietoa, jota ei ole kirjattu ylös ja tuoda esiin uusia näkökulmia, joita voidaan hyödyntää turvasuunnittelussa. Tietoriskien kartoituksessa miellekarttaa voidaan hyödyntää käyttämällä kolmivaiheista tarkastelua, jonka kautta yritetään ryhmässä tunnistaa tietojärjestelmiin kohdistuvat riskit, löytää ratkaisut riskien minimoimiseksi ja pohtia varotoimia riskin realisoituessa. Miellekartan tekeminen tulee aloittaa määrittämällä käytettävät kuvaustavat ja jaottelu. Tarkoitus on muodostaa mahdollisimman kattava poikkileikkaus henkilöstöstä, jonka kanssa etsitään riskejä ja uhkakuvia. Ensimmäisessä vaiheessa kirjataan ylös jo realisoituneita riskejä, seuraavaksi pohditaan todennäköisiä ja oletettavia riskejä ja kirjataan nämä miellekarttaan. Riskikartoitus voidaan tarpeen mukaan kohdistaa yksittäiseen prosessiin, tietojärjestelmään tai mahdollisesti koko organisaatioon. Miellekarttoja käyttämällä on mahdollista muodostaa jäsennetty kuva tietoturvallisuuden kokonaistilanteesta. (Hakala ym. 2006, 29–31.)

Baseline-menetelmä (Baseline Method) perustuu ”asianmukaisen huolellisuuden noudattamisen” – periaatteeseen. Baseline-menetelmä itsessään ei ole monimutkainen käyttää ja se voi olla toimiva ratkaisu monille organisaatioille, jotka aloittavat tietoriskienhallintaa. Metodin soveltamisen esitietovaatimuksena on kohteen peruskontrollien tunteminen, jotta niitä on mahdollista arvioida ja soveltaa tarvittaessa. (Kajava & Siponen 2002, 3–4.) Kohteet suojataan ensisijaisesti kohteiden omilla suojauskeinoilla, joita myös muut organisaatiot käyttävät omissa liiketoiminnoissaan. Näitä hyväksi havaittuja menetelmiä kutsutaan peruskontrolleiksi (Baseline Controls). (Miettinen & Kajava 1994, 18–19.)

Baseline-menetelmässä aluksi määritetään suojattava kohde tai kohteet. Seuraavaksi tunnistetaan kohteiden olemassa olevat suojaukset eli kontrollit. Olemassa olevista suojauksista valitaan peruskontrollit, joiden avulla voidaan torjua yleisimmät uhat. (Miettinen & Kajava 1994, 18–19). Peruskontrollien käyttöönoton jälkeen keskitytään mahdollisiin kohdetta uhkaaviin erityisuhkiin. Ensin tunnistetaan mahdollisimman monia erityisuhkia ja arvioidaan riskien todennäköisyys ja vakavuus. Tämän jälkeen analysoidaan lisäkontrollit, joilla voidaan hallita ja minimoida erityisuhkia. Kun lisäkontrollit on määritetty, laaditaan toteutussuunnitelma niiden käyttöönotosta. Hyväksytään ja toteutetaan määritetyt lisäkontrollit. Säännöllinen turvallisuuden seuraaminen on tärkeä osa Baseline menetelmää, koska itse kontrollien käyttöönotto ei poista uhkia vaan pienentää uhkien toteutumisen todennäköisyyttä. (Miettinen & Kajava 1994, 18–19).

Potentiaalisten ongelmien analyysi (POA) soveltuu hyvin monien erilaisten ongelmien analysointityökaluksi. POA on yksinkertainen menetelmä, joka perustuu tarkistuslistoihin. Ensimmäinen toimenpide on projektiryhmän kokoaminen, jonka jäsenet valitaan tarkasteltavan kohteen perusteella. Kaikista tarkastelukohteeseen vaikuttavista henkilöstöryhmistä tulee olla osallistuja. Tärkeimmät henkilöt ovat kohteen toiminnasta vastaavat henkilöt, perustason käyttäjät, erityisalueiden asiantuntijat ja johdon asiantuntija. Johdon osallistuminen on tärkeää, koska vain johdolla on tieto käytettävissä olevista resursseista. Johdon edustaja toimii myös ryhmän puheenjohtajana. Työryhmässä on tarpeellista olla myös sihteeri, joka hankkii taustatietoja ja koordinoi prosessia. (VTT Potentiaalisten ongelmien analyysi.)

Potentiaalisten ongelmien arvioinnin aloittaa sihteeri ideointilomakkeen laatimisella ja tarkastusalueen avainsanaluettelon määrittämisellä. Sihteeri valitsee tarkasteltavan kohteen ja rajaa arviointiin kohdistuvan alueen, jotta vältetään pintapuoliset arvioinnit. Taustaselvityksen jälkeen puheenjohtaja käy järjestelmällisesti läpi kohteeseen kohdistuvat riskit sihteerin laatimien listojen avulla. Tavoitteena on löytää suurimmat ja keskeisimmät riskit. Työryhmä työskentelee aluksi itsenäisesti käymällä listat läpi ja listaten samalla ryhmän mielestä kohdetta koskevat riskit. Kaikkien tulisi listata kolmesta viiteen ongelma- tai riskitilannetta. Seuraavaksi listoja kierrätetään ja ryhmän jäsenet lisäävät tai täydentävät muiden tekemiä tilannekuvauksia. Tämä vaihe voidaan tehdä myös sähköisesti. Listojen ollessa valmiita käydään jokainen kohta yksitellen läpi ryhmässä keskustellen. (Leppänen 2006, 140–143.) Tässä vaiheessa keskitytään ongelma- ja riskitilanteiden löytämiseen, eikä tarkoituksena ole vielä kehittää toimenpiteitä riskien ehkäisemiseksi. Työryhmän sihteeri tekee listoista yhteenvedon, johon tehdään alustava ongelmatilanteiden kokoaminen ja luokittelu. (VTT Potentiaalisten ongelmien analyysi.)

Ongelmat luokitellaan kolmeen luokkaan: A) Riskit, jotka edellyttävät jatkokäsittelyä. Nämä siirretään arviointivaiheeseen. B) Jo tiedostetut ja luotettavasti hoidossa olevat riskit, joille määritetään vastuuhenkilö. C) Riskit, jotka ovat merkityksettömiä liiketoiminnalle tai riskit, joiden hallitseminen on joko mahdotonta tai kannattamatonta. Kannattamattomuudella voidaan esimerkiksi tarkoittaa riskiä, jonka hallitseminen tulisi kalliimmaksi kuin itse riskin toteutuminen. (Leppänen 2006, 142.)

4.2 Standardit

Tietoturvasuunnitteluun on kehitetty kansainvälisiä ja kansallisia tietoturvastandardeja. Tietoturvastandardit eivät aseta vaatimuksia tietoturvan tasolle ja sisällölle vaan keskittyvät suunnittelussa käytettäviin menettelytapoihin. Standardit tarjoavat selkeän ja vertailukelpoisen rakenteen tietoturvasuunnitelmassa syntyville dokumenteille. Julkisyhteisöjen tietoturvallisuuden kehittäminen ja valvonta on valtionvarainministeriön vastuulla ja käytännön ohjeistuksen toteuttaa viestintävirasto. (Hakala ym. 2006, 46.)

Yrityksille, säätiöille, yhdistyksille sekä julkisyhteisöille soveltuvat yleisluontoiset standardit, kuten ISO 17799 ja ISO 27001. ISO 17799 -standardi on menettelytapaohje (code of practise). Siinä määritellään osa-alueet, jotka on huomioitava tietoturvallisuuden suunnittelussa, ylläpidossa ja kehittämisessä. Se kuvaa turvallisuuden parantamiseen tähtäävien toimenpiteiden käynnistämisen, toteuttamisen sekä tietoturvallisuushallinnon ylläpitämisen ja kehittämisen. Standardi toimii yleisohjeena yrityksen omien tietoturvakäytäntöjen laadintaan. Lisäksi sitä voi käyttää olemassa olevien tietoturvakäytäntöjen arviointiin. ISO 27001 -standardin tavoitteena on puolestaan määritellä tietoturvallisuuden hallinnan malli. Standardi käsittää sen perustamisen, käyttöönoton, käyttämisen, ylläpidon, valvonnan, katselmusten ja käsittämisen perusteet. Standardi perustuu tietoturvallisuuden hallinnan mallin prosessinomaiseen kehittämiseen PDCA-mallin (Plan, Do, Check, Act) mukaisesti. (Hakala ym. 2006, 46-49.)

5 PK-YRITYKSEN RISKIENTUNNISTAMINEN

5.1 Tietoriskianalyysin toteuttamisen tarpeet

Tietoriskianalyysi tuli ajankohtaiseksi, kun tietohallinnon päivittäisessä toiminnassa tuli esille toistuvia epäselvyyksiä jo käytössä olevissa prosesseissa ja prosessimäärityksissä. Yhdeksi ongelmaksi identifioitiin sisäinen tiedottaminen. Edellä mainittujen seikkojen vuoksi tietohallinnossa katsottiin tarpeelliseksi lisätä tietohallinnon prosessien läpinäkyvyyttä ja arvioida prosessien kokonaisvaltaista toteutusta. Tietohallinnon prosessit haluttiin selkiyttää yrityksen ylimmälle johdolle, henkilöstöhallinnolle, esimiehille ja henkilökunnalle. Projektin suurimpana haasteena oli avainhenkilöiden motivointi projektiin osallistumiseen, koska toimeksianto tuli tietohallinnon sisältä, ei ylimmältä johdolta.

Tietoriskianalyysi todettiin hyväksi tavaksi aloittaa keskustelu tietoturvallisuudesta. Tietoturvallisuuden merkityksen ymmärtäminen koko yrityksen henkilökunnan laajuisesti on välttämätöntä, jotta tietoturvallisuus toteutuu kokonaisuudessaan yrityksen toiminnassa. Tietoturvallisuuden edistäminen ja hallinnointi päätettiin aloittaa henkilöstön tietoturvatietoisuutta kehittämällä.

Yrityksessä ei ollut aikaisemmin arvioitu tietoriskejä osana liiketoimintaa. Yrityksestä puuttui kokonaisvaltainen tietoturvallisuuspolitiikka ja käytössä oli lukuisia erillisiä prosesseja ja politiikkoja, joiden määrittelemiseen ja hallinnoimiseen olivat osallistuneet eri tahot. Yrityksen henkilöstön suhteellisen suuri vaihtuvuus ja kasvu lisäsivät hallinnan, koulutuksen ja tiedottamisen tarvetta.

Vaikka tietoriskianalyysi käynnistettiin tietohallinnossa, ensisijaisena lähtökohdaksi sille asetettiin, että tietohallinto ei voi, eikä sen tule toimia yksinään yrityksen tietoturvallisuuden kehittäjänä. Tietoturvallisuus on yrityksen kaikkien toimintayksiköiden asia ja se on oleellisessa osassa lukuisissa yrityksen sisäisissä ja ulkoisissa prosesseissa. Tietohallinnon omat prosessit sidottiin kuitenkin luonnollisesti tietoturvallisuuden kehittämiseen ja hallintaan.

5.2 Projektin ja case-tutkimukseni aloitus ja sen tavoitteiden määrittely

Yrityksen tietoriskianalyysi jaettiin kahteen erilliseen vaiheeseen: 1) Suomen liiketoimintojen tietoriskianalyysi ja 2) ulkomaan liiketoimintojen tietoriskianalyysi. Tämän opinnäytetyön tutkimus – yrityksen Suomen liiketoimintojen tietoriskianalyysi - määriteltiin toteutettavaksi ajalla 1.8.2010 – 31.11.2010. Yrityksen tietoriskianalyysin toista vaihetta ei vielä aikataulutettu.

Henkilökohtaisena haasteena koin projektin laajuuden - en ollut aikaisemmin johtanut yhtä laajaa yrityksen sisäistä kehitysprojektia. Pidin tietoriskianalyysin toteuttamista, aineiston keruuta, haastateltavien osallistuttamista ja aineiston analysointia hyvin vaativana. Tutkimukseni alkuvaiheessa tietoturvan ja riskien hallinta olivat minulle vain pintapuolisesti tuttuja käsitteitä, joten aiheeseen syventymiseen ja sopivan tutkimusmenetelmän valitsemiseen oli varattava riittävästi aikaa.

Tutkimukseni teoreettinen viitekehys pohjautui kirjastoista, elektronisista tietolähteistä ja alan lehdistä löytämääni lähdekirjallisuuteen. Motivaationi sopivan lähdekirjallisuuden hakemiseen ja lukemiseen oli korkea. Kolmen vuoden työkokemukseni tietohallinnon eri tehtävistä tarjosi lukemaani tartuntapintoja työelämän hyviin ja huonoihin käytäntöihin.

Tietoriskianalyysille määritettiin kolme tavoitetta: 1) Johdon tietoriskitietoisuuden kehittäminen, 2) tämän hetkisten vastuualuiden ja prosessien omistajien kartoittaminen sekä 3) tietoturvan kehittämistarpeiden kartoittaminen liiketoiminnan näkökulmasta.

Johdon tietoriskitietoisuuden kehittämisen lähtökohtana oli lisätä tietohallinnon prosessien läpinäkyvyyttä - saada ne yrityksen jokaisella tasolla ymmärrettäviksi ja osaksi jokapäiväistä liiketoimintaa. Tämän tavoitteen saavuttamiseksi oli ensisijaisen tärkeää osallistuttaa ja sitouttaa yrityksen avainhenkilöt tietoturvariskien ja tarpeiden arvioimiseen. Henkilöstön osallistuttaminen tietoriskianalyysiin oletettavasti lisää yrityksen henkilöstön ymmärrystä tietoturvasta ja sen merkityksestä. Samalla yrityksessä voidaan huomata, että tietoturva ja sen kehittäminen ei ole vain erillinen jonkin yksittäisen yksikön huolenaihe vaan koko yrityksen ja henkilöstön toimintaan liittyvä asia.

Vastuualueiden ja prosessien omistajien kartoitus oli tutkimani nopeasti kasvaneen yrityksen kohdalla hyvin tärkeää – oletusarvo oli, että vastuualueet ja prosessien omistajat saattavat olla epäselviä. Yrityksessä osallistuu monia tahoja tietoturvallisuuteen liittyvien prosessien hallintaan. Tämä lisää päällekkäistä työtä ja mahdollistaa epäselvyyksiä prosesseissa. Tavoitteena oli pyrkiä löytämään päällekkäiset prosessit, pyrkiä karsimaan päällekkäisyyksiä ja selkeyttämään vastuualueet sekä standardoida prosesseja.

Tietoturvan kehittämistarpeiden kartoittaminen liiketoiminnan näkökulmasta oli välttämätöntä, jotta tietoturvan kehittämisen priorisointi voitaisiin asettaa liiketoiminnan vaatimusten mukaiseksi. Pitkän aikavälin tavoitteena oli pystyä jäsentämään ja raportoimaan systemaattisesti tietoa tietoriskeistä ja niiden hallinnasta johdolle päätöksenteon tueksi. Johdon rooli tietoturvan kehittämisessä on merkittävä - johto sitouttaa myös muun henkilökunnan noudattamaan hyväksi koettuja prosesseja.

Tietoriskianalyysiprojektiryhmään valittiin yrityksen ylin johto, linjaesimiehet, kaksi avainasemassa olevaa asiantuntijaa ja yksi projektipäällikkö. Projektiryhmä käsitti yhteensä 10 henkilöä yrityksen Suomen toimipisteessä. Projektiryhmän jäsenet kattoivat kaikki yrityksen liiketoiminnan osa-alueet. Projektin johtaminen ja materiaalin kokoaminen jäivät vastuulleni yrityksen tietohallintojohtajan avustuksella.

5.3 Tietoturvariskien arvioinnin lähestymistavan määrittäminen

Sopivan lähestymistavan määrittäminen tietoturvariskien arviointiin oli erittäin haastavaa. Yrityksen tietoturvariskien arvioinnin potentiaalisiksi vaihtoehdoiksi määrittelin seuraavat lähestymistavat: MindMap-, POA-, skenaarioanalyysi- ja tarkistuslistamenetelmä.

Lähestymistavaksi valittiin tarkistuslistat, koska ne ovat nopeita laatia ja niiden läpikäyminen on huomattavasti nopeampaa kuin muiden potentiaalisten lähestymistapojen. Yrityksessä ei ennestään ollut kokemusta tietoriskien arvioinnista, eikä arviointia ollut toteutettu yrityksessä aikaisemmin. Muiden arviointimenetelmien käyttäminen olisi vaatinut huomattavasti mittavampia alkuselvittelyjä ja valmisteluja. Todennäköistä oli myös, että yrityksen johdon kiirellisyyden vuoksi sitouttaminen eräiden menetelmien lukuisiin palavereihin olisi ollut haastavaa.

Tarkistuslistojen heikkoudet - liiallisessa yleisluontoisuudessa ja uusien uhkien etsimisessä - huomioitiin mentelmää valittaessa. Tietoriskien arviointiin päätettiin kehittää yrityksen toiminnan mukainen ja käsiteltävät asiat sisältävä räätälöity tarkistuslista. Arvioinnin tavoitteena ei myöskään ollut pyrkiä löytämään mahdollisimman paljon uhkia vaan käynnistämään yrityksessä pitkäkestoinen riskienhallintaprosessi.

Tarkistuslistoja ei kannattanut laatia alusta alkaen itse, vaan oli järkevää käyttää pohjana valmiita kysymyslistoja. Projektissa päädyin käyttämään PK-RH:n (PK-RH 2010) tarjoamia pk-yrityksille suunnattuja tietoturvariskien tarkistuslistoja.

Tavoitteenani oli kehittää yrityksen toimintaan räätälöity ja helppokäyttöinen tarkistuslista, jonka käyttäminen ei edellyttäisi tietoteknistä tietämystä. Aloitin yrityksen tarpeisiin sopivan tarkistuslistan kehittämisen karsimalla valitsemastani PK-RH:n tarkistuslistasta kaikki kysymykset, jotka koin epäoleellisiksi tarkastelemani yrityksen liiketoiminnan kannalta. Jäsentelin kysymyksiä yrityksen toimintaan ja asetettuihin tavoitteisiin sopivaksi.

Esittelin kehittämäni tarkistuslistan yksityiskohtaisesti yrityksen tietohallintajohtajalle. Katselmoinnin perusteella rajasin kysymysten määrää tarkistuslistassa edelleen – siten että se sisälsi enää ainoastaan kaikista oleellisimmiksi katsomamme kysymykset. Lopullisen tarkistuslistan kysymykset jäsentyivät neljään osa-alueeseen: johdon tietoisuus, toimitilojenturvallisuus, tietojärjestelmien suojaus ja henkilöstön tietoisuus ja toiminta.

Kysymysten muotoilussa pyrin mahdollisimman ei-teknisiin ilmaisuihin, jotta kyselyn käyttäjä voisi keskittyä tietoteknisten yksityiskohtien sijaan arvioimaan tietoriskejä oman roolinsa kautta. Tällä periaatteella karsin tarkistuslistasta myös pois teknisiä osa-alueita. Esimerkiksi tarkistuslistani ”tietojärjestelmien suojaus”-osuus sisältää ainoastaan ”tietojärjestelmien käyttöperiaatteet” - ei teknisiä osa-alueita, kuten ”teknisen ympäristön hallintaa ja valvontaa”, ”teknisten järjestelmien hankintoja”, ”huoltoa”, ”muutoksia ja poistoja käytöstä”, ”ohjelmistoja”, ”teknisiä suojaamiskeinoja” ja ”palveluita”. PK-RH:n tarkistuslistamallista karsitut tekniset osa-alueet käsiteltiin tietohallintoyksikössä sisäisesti.

PK-RH:n tarkistuslistat eivät mielestäni soveltuneet tietojärjestelmien tietoriskien arviointiin erityisen hyvin niiden yleisluontoisuuden takia. Tosin on todettava, että tarkistuslistat olisivat varmasti toimiva tapa aloittaa tietojärjestelmien tietoriskien arviointi yrityksessä, jossa ei ole riittävää tietojärjestelmien osaamista, koska listat käsittelevät erittäin kattavasti perusasiat.

5.4 Sähköisen kyselylomakkeen luominen tarkistuslistasta ja kyselyn toteutus

Tarkistuslistakysely oli tarkoitus toteuttaa ensin strukturoituna henkilökohtaisena teemahaastatteluna. Päädyin kuitenkin toteuttamaan sen vielä rakenteellisemmin – verkkopohjaisena kyselylomakkeena. Valintaan vaikutti vastaajien suuri määrä sekä ajatus käyttää samaa sähköistä tarkistuslistakyselyä myös yrityksen ulkomailla sijaitsevien toimipisteiden tietoturvallisuuden arvioinnissa.

Verkkopohjaisen kyselyn toteuttamisessa oli selvästi omat heikkoutensa, mutta myös vahvuutensa. Verkkopohjainen kysely ei tarjonnut yhtä hyvää kehystä avoimelle keskustelulle kuin avoin teemahaastattelu – on oletettavaa, että osa riskeistä saattoi jäädä tiiviin rakenteellisessa kyselyssä huomiotta. Tuloksena saattaa olla pintapuolinen yhteenveto. Toisaalta tulosten verrattavuus on nopeaa, ja itse analyysin läpivienti nopeutuu huomattavasti. Kyselyä on myös mahdollista hyödyntää uudelleen, ja saatuja tuloksia voidaan verrata helposti edeltävään kyselyyn.

Koska kysely toteutettiin verkkopohjaisesti kyselylomakkeena haastatteluiden sijasta, päädyin muuttamaan kysymysten asettelua – tarkistuslistan kysymysten sijaan esitin kyselylomakkeessa väittämiä. Pyrin muodostamaan väittämistä mahdollisimman neutraaleja, jotta väittämät eivät johdattelisi vastaajaa. Monet PK-HR:n alkuperäiset kysymykset esittivät yhdessä kysymyksessä kaksi eri asiaa. Muuttaessani kysymyksiä väittämiksi oli huomioitava, että väittämät eivät saa sisältää kahta väitettä. Kyselyni kuusi luokkaiseen Likert-asteikkoon perustuvat vastausvaihtoehdot eivät toimivia, jos väitteessä on kaksi väitettä. Samassa yhteydessä kun kysymykset yksinkertaistettiin väittämiksi, käännettiin ne myös englanniksi, joka on yrityksen liiketoimintakieli.

Kyselylomakkeen väitteet käsittelevät tietoturvan perusasioita. Väitteiden ja niihin liitettyjen kysymysten avulla kysytään vastaajalta esimerkki 1 mukaisesti: 1) onko väittämän esittämät asiat hallinnassa, 2) miten tärkeäksi vastaaja kokee väittämässä esitetyn asian liiketoiminnan kannalta, ja 3) kenen vastuulla vastaaja kokee väittämässä esitetyn asian yrityksessä kuuluvan?

---

1. Business critical information is identified in organization.

1. How much you agree or disagree:
    a. Strongly Agree
    b. Agree
    c. Not Agree or Disagree
    d. Disagree
    e. Strongly Disagree
    f. I am not aware of it

2. How important it is for business:
    a. Very important
    b. Important
    c. Neither agree nor disagree
    d. Moderately important
    e. Unimportant
    f. I am not aware of it

3. Who is the responsible of it:
    a. Chief of business management (CEO, managing director, COO)
    b. Chief of finance
    c. Chief of human resources
    d. Chief of IT
    e. Chief of office administration
    f. Chief of department
    g. Other:_____
    h. I am not aware of it

Esimerkki1. Kyselylomakkeen ensimmäinen kysymys.

Esimerkki 1 ensimmäisen väittämän kysymyksen tavoitteena on selvittää, onko väitteessä mainittu prosessi tai asia yrityksessä jo hallinnassa. Vastauksista voidaan myös päätellä, ovatko vastaajat tietoisia jo olemassa olevista prosesseista. Väittämän esittämän prosessin voidaan olettaa olevan yrityksessä hallinnassa, mikäli sekä asianomaisen prosessin omistaja että muut vastaajat vastaavat olevansa väittämän kanssa samaa mieltä (”Strongly agree” tai ”Agree”). Hajonta vastauksissa voi olla osoitus esimerkiksi väitteen esittämän soveltamisen ja käyttöönoton, yrityksen viestinnän tai henkilöstön koulutuksen puutteellisuudesta.

Väittämän toisen kysymyksen tavoitteena on selvittää, väittämän esittämän prosessin/asian merkitys yrityksen liiketoinnassa. Vastauksia voidaan käyttää avuksi tietoturvakehityskohteiden priorisoinnissa – liiketoiminnan kannalta tärkeiden asioiden/prosessien tietoturvan kehittäminen on luonnollisesti kannattavinta. Vastausten avulla voidaan luoda yrityksen liiketoiminnan priorisoima alustava etenemissuunnitelma tietoturvan kehittämiseen.

Väittämän kolmannen kysymyksen tavoitteena on tarkentaa henkilöstön vastuualuita yrityksessä. Vastauksista voidaan tulkita vastaajien käsityksiä henkilöstön vastuualueista suhteessa väittämässä esitettyihin prosesseihin - onko olemassa olevien prosessien omistajuus yksiselitteistä. Vastauksista voidaan tehdä myös karkea arviointi eri tahojen osallistumisesta väittämien mainitsemiin prosesseihin – ja mahdollisesti löytää päällekkäisyyksiä. Päällekkäiset prosessit voidaan mahdollisesti tulevaisuudessa järjestää vain yhden tahon hallittaviksi. Vastausvaihtoehtona kolmannessa kysymyksessä on myös avoin vastauskenttä ”Other”, johon vastaaja voi syöttää vaihtoehdon, jota ei ole valittavissa.

Jokaisessa kysymyksessä viimeisenä vaihtoehtona on: ”I am not aware of it”. On todennäköistä, että kukaan vastaajista ei ole tietoinen yrityksen kaikista liiketoiminnan osa-alueista ja sisäisistä prosesseista. Tämä vastausvaihtoehto vähentää vastaajien arvailua prosessien tilasta, omistajuudesta tai vastuuhenkilöstä. Näin on mahdollista saada myös kokonaisvaltaisempi kuva yrityksen henkilöstön tietoisuudesta väittämissä mainituista prosesseista.

Työkaluksi verkkokyselyn toteuttamiseen valitsin Webropol-verkkokyselyohjelmiston (Webropol 2010). Ohjelmisto mahdollisti yhteen väittämään useamman kysymyksen liittämisen. Jaoin sähköisen kyselylomakkeen neljään erilliseen osa-alueeseen: johdon tietoisuus, toimitilaturvallisuus, tietojärjestelmien suojaaminen ja henkilöstön tietoisuus ja koulutus. Jokaisen osa-alueen lopussa vastaajan oli mahdollista kirjoittaa mieleen tulleita huomioita avoimeen tekstikenttään.

Ennen kyselyn toteuttamista kyselyn ymmärrettävyyttä ja kysymysten toimivuutta oli testattava. Ensimmäisen testauksen suoritti tietohallintojohtaja. Testauksen jälkeen lukuisia kysymyksiä tarkennettiin ja muutama päällekkäinen kysymys poistettiin. Tämän jälkeen tietohallintojohtaja teki kyselyn uudelleen. Kun kysely oli todettu toimivaksi, valitsin projektiryhmästä testikyselyyn kolme eri tehtävissä toimivaa henkilöä (talous-, henkilöstö-, ja AV-tuotantojohtaja).

Testien tarkoituksena oli arvioida kysymysten ymmärrettävyys, kattavuus, tarkoituksenmukaisuus ja kyselyn kesto. Käytyäni kyselyn henkilökohtaisesti testihenkilöiden kanssa läpi päädyin tulokseen, että kyselylomakkeen täyttäminen tarvitsee tuekseen henkilökohtaista tukea. Tutkijan paikalla oleminen varmisti vastausten saamisen aikataulun mukaisesti ja kahdenkeskiset kyselyt mahdollistivat keskustelut, joiden kautta sain paljon hyödyllistä lisäinformaatiota. Vaikka kysely ei ollut tekninen, niin testivastaajat toivoivat joihinkin kohtiin tarkennusta ja esimerkkejä. Jokainen testivastaaja myös totesi, että paikalla oloni oli ollut hyödyksi - kysely tuli tehtyä niin ”tosissaan eikä hätiköiden”. Osa kyselylomakkeen väittämistä oli myös haastavia, ja vastaaja olisi turhautunut nopeasti ilman tarvittavia tarkennuksia.

Testihenkilöiden jälkeen sovin henkilökohtaisesti projektiryhmän kuuden muun henkilön kanssa ajan kyselyn toteuttamiseksi. Varasin henkilöiltä kasvokkain ohjeistettua kyselylomakkeen täyttämistä varten kaksi tuntia aikaa. Keskimäärin testihenkilöt olivat käyttäneet aikaa 90 minuuttia kyselyn tekemiseen. Pisin testihenkilön käyttämä aika kyselyn täyttämiseen oli 157 minuuttia ja lyhyin 45 minuuttia. Tavoitteeni oli toimia jokaisessa kyselyssä väittämiin nähden neutraalina ja olla näin vaikuttamatta vastaajien vastauksiin. Vastaajien pyytäessä esimerkkejä pyrin antamaan lähinnä esimerkkejä - uhkista jossain kuvitteellisessa yrityksessä, en case-yrityksessä. Vastaajat taas kuvasivat kyselylomaketta tehdessään ja keskustellessaan riskejä nimenomaan case-yrityksessä - kirjasin kaikki vastaajien huomiot analyysiani varten. Keskimääräinen kyselylomakkeen täyttöaika ja siihen liittyvä keskustelu oli vastaajaa kohti 78 minuuttia – tämä oli suhteellisen lähelle alun perin arvioimaani 60 minuutin vastausaikaa.

6 AINEISTO JA SEN ANALYSOINTI

Tutkimusaineistoni koostuu kyselylomakkeen vastauksista ja kyselylomakkeen ohessa tekemistäni keskustelumuistiinpanoista – kymmenen henkilön kanssa.

Lähestyin keräämääni aineistoa kyselylomakkeeni neljästä eri aihealueesta tai kategoriasta: johdon tietoisuus, toimintaympäristön, työ- ja palvelutilojen turvallisuuden kehityskohteet, tietojärjestelmien suojaus ja henkilöstön tietoisuus ja toimintatavat. Kyselytilanteessa tekemieni keskustelumuistiinpanojen pohjalta loin tutkimukseeni yhden lisäkategorian: ”liiketoiminnan kehittämistarpeet tietoturvallisuuden toteuttamiseksi”. Kokosin siihen kaikki kehittämiskohteet, joita vastaajat sivusivat kyselyä täyttäessään. Analysoimani aineisto koostui siis kyselylomakkeen vastauksista Loin aineistoni analyysissa jokaisesta kategoriasta oman taulukkonsa. Taulukoissa on seuraavat tiedot: Kehityskohde – Ongelman kuvaus – Prioriteetti ja – Toimenpiteet. Taulukoiden prioriteetin määritys perustui siihen, kuinka moni vastaaja koki väitteen liiketoiminnan kannalta ”tärkeäksi” tai ”erittäin tärkeäksi”.

Määrittelin esitetyissä taulukoissa kehityskohteen prioriteetin ”Melko tärkeäksi”, mikäli viisi tai kuusi vastaajaa koki kyselylomakkeessa esitetyn väitteen ”tärkeäksi” tai ”erittäin tärkeäksi”. ”Tärkeäksi”, mikäli seitsemän tai kahdeksan vastaajaa koki esitetyn väitteen ”tärkeäksi” tai ”erittäin tärkeäksi”. ”Erittäin tärkeäksi”, mikäli yhdeksän tai kymmenen vastaajaa koki esitetyn väitteen ”tärkeäksi” tai ”erittäin tärkeäksi”. Mikäli ”tärkeä” tai ”erittäin tärkeä” vastauksia oli väitteeseen vähemmän kuin viisi, kehityskohteen prioriteetti on taulukoissa ”Ei tärkeä”. Taulukot sisältävät lisäksi kehityskohteita, joille ei ole määritetty priorisointiarvoa. Näistä ei ole esitetty väittämiä kyselylomakkeessa. Nämä kehityskohteet tulivat esille keskusteluissa vastaajien kanssa.

6.1 Johdon tietoisuus

Taulukko 2 Johdon tietoisuuden kehityskohteet

Kehityskohde	Ongelman kuvaus	Prioriteetti	Toimenpiteet
Liiketoimintakriittisen tiedon tunnistaminen ja hallitseminen	Liiketoimintakriittistä tietoa ei ole tunnistettu ja tarvittavaa tietoa ei ole aina saatavilla	Erittäin tärkeä	Projektiryhmän kokoaminen tiedon tunnistamista varten
Tiedon suojaaminen uhkilta. (tulipalot ja vesivahingot)	Ei ole kartoitettu mahdollisia uhkia.	Erittäin tärkeä	Uhkien tunnistaminen, arviointi ja toimenpiteiden määrittäminen.
Tietosuoja käytäntöjen selkeyttäminen	Tietosuoja huomioidaan henkilöstöhallinnassa, mutta ei koko yrityksessä.	Erittäin tärkeä	Yhteisen tietosuoja käytännön laatiminen
Tietoturvan kehittämiseen on varattu riittävät resurssit	Tietoturvan kokonaisvaltaista kehittämistä varten ei ole tällä hetkellä tiettyä vastuullista henkilöä tai tahoa	Erittäin tärkeä	Vastuuttaa tietoturvan kokonaisvaltainen kehittäminen yhdelle taholle.

Johdon tietoisuus-osion väittämien avulla pyrin kartoittamaan johdon tietoisuutta liiketoimintakriittisen tiedon hallinnasta, tietosuojan noudattamisesta ja riittävien resurssien varaamisesta tietoturvan kehittämiseksi, nämä asiat on esitetty taulukossa 2. Ensimmäisenä selvitin, onko liiketoiminnalle kriittinen tieto tunnistettu ja onko johto tietoinen liiketoimintakriittisestä tiedosta. Kuusi vastaajista oli sitä mieltä, että liiketoimintakriittistä tietoa ei ole tunnistettu yrityksessä. Ainoastaan kaksi vastaajaa oli väittämän kanssa samaa mieltä. He rajasivat kysymyksen omaan toimialueensa – ja kokivat siihen liittyvän liiketoimintakriittisen tiedon olevan tunnistettua ja hallittua. Kaikki vastaajat näkivät tämän tärkeäksi liiketoiminnan kannalta. Ylimmän johdon koki kuusi vastaajaa vastuulliseksi tahoksi väittämälle ja kolme vastaajaa koki, että vastuu tulisi olla esimiehillä tai mahdollisella projektiryhmällä. Perusteena oli, että esimiesten tulisi dokumentoida oman yksikkönsä toiminnan liiketoimintakriittinen tieto. Neljä vastaajaa koki, etteivät he ole työssään tietoisia liiketoimintakriittisestä tiedosta. Yleisin toteamus väitteeseen oli vastakysymys: ”*Mitä on liiketoimintakriittinen tieto*?” Tämä on yrityksen kannalta ongelmallista ottaen huomioon haastateltavien avainaseman organisaatiossa. Yksi vastaaja tiivisti liiketoimintakriittisen tiedon tunnistamisen tärkeyden seuraavasti: *”Asiakastieto on liiketoimintakriittistä tietoa, joka on dokumentoitu CRM (Customer Relationship Management) järjestelmään, jolloin asiakastieto ei ole kenenkään henkilön omaisuutta vaan yrityksen omaisuutta.”*

Tiedon tunnistamisessa nähtiin kuitenkin seuraava ongelma: *”Liiketoiminnalle kriittinen tieto on identifioitu Suomessa, mutta ei ulkomailla, jolloin tapahtuu ’Lost in translation’ ilmiö. Käännökset saattavat poiketa huomattavasti alkuperäisistä dokumentaatioista. Ulkomailta saatava tieto ei ole luotettavaa.*” Liiketoimintakriittisen tiedon tunnistamisen puute tulee esiin myös tiedon heikkona saatavuutena: ”*Ihmiset haluaa tehdä työnsä hyvin, mutta aina ei ole tietoa saatavilla tarkoitusperistä ja miten työ tulisi suorittaa*”. Liiketoimintakriittiseen tietoon liittyen yrityksessä ei oltu huomioitu uhkaavia tilanteita, jotka voisivat tuhota yritykselle liiketoimintakriittisen tiedon, kuten tulipalo tai vesivahingot.

Tietosuojan vastaajat kokivat olevan hyvin hoidettu organisaatiossa. Kyselyn aikana tuli kuitenkin esille, että tietosuojan huomioiminen koko organisaation toiminnassa on puutteellista. Esimerkiksi henkilöitä, jotka vastaavat rekrytoinneista, ei ole ohjeistettu huomioimaan tietosuojaa työssään. Tietosuojasta vastuullisen tahon nimeäminen oli myös vaikeaa vastaajille. Kymmenen henkilön otannassani tietosuojaväittämä oli vastuutettu kuudelle eri taholle. Yrityksen vastuu tietosuojan hallinnasta ei näin oletettavasti ole yrityksen johdolle selvä.

Johdon tietoisuuteen liittyen kysyin, onko tietoturvallisuuden kehittämiseen varattu resursseja, ja mikä on yrityksen johdon käsitys siitä vastuussa olevasta tahosta. Viisi vastaajista koki, että yrityksessä on vastuullistettu taho tietoturvan kehittämiseen. Neljä vastaajaa oli väitteen kanssa eri mieltä. Kuusi vastaajista koki vastuulliseksi tahoksi tietohallinnon. Tietohallinnosta kyselyyn vastasi kolme henkilöä ja he kaikki kokivat, että tietoturvallisuudelle ei ole vastuutettu yhtä tiettyä tahoa. Näkemysero todennäköisesti johtuu tietoturvan käsitteen erilaisesta tulkinnasta.

Johdon tietoisuus-osion perusteella ehdottaisin seuraavia kehitystoimenpiteitä. Pitäisi perustaa koko organisaation kattava yhteinen tietosuojakäytäntö, joka on dokumentoituna ja henkilökunnan saatavilla. Tämä takaa yhteisen toimintamallin ja samalla yrityksen vastuu on selkeä henkilökunnalle. Tiedon liiketoimintakriittisyyttä tulisi arvioida johtoryhmässä ja päättää tarpeelliset toimenpiteet sen tunnistamiseksi, suojaamiseksi ja hallitsemiseksi. Vastuullinen taho tietoturvan kehittämiseen tulisi nimetä. Tämän tahon tulisi toimia eri sidosryhmien kanssa tietoturvan kehittämiseksi ja samalla raportoida johdolle, jotta tietoturva voitaisiin huomioida paremmin päätöksenteossa. Johdon tarvitsemasta tiedosta tulisi määrittää, mikä tieto on oleellista päätöksenteolle. Tietoturvan kehittämisen vastuullistamisen lisäksi tulisi huomioida, että vastuullisella taholla on aikaa ja resursseja huolehtia tietoturvan kokonaisvaltaisesta kehittämisestä.

6.2 Toimintaympäristön, työ- ja palvelutilojen turvallisuus

Taulukko 3 Toimintaympäristön, työ- ja palvelutilojen turvallisuuden kehityskohteet

Kehityskohde	**Ongelman kuvaus**	**Prioriteetti**	**Toimenpiteet**
Neuvotteluhuoneiden siistiminen	Toisinaan neuvotteluhuoneissa on edellisten kokouksien jäljiltä muistiinpanoja ja papereita	Erittäin tärkeä	Tulee määritellä kokous- ja vieraskäytäntö, joka on suunnattu kutsujille
Rakennuksen turvallisuus	Pääsynvalvonta ei ole päiväsaikaan luotettava	Tärkeä	Huomauttaa ja vaatia taloyhtiöltä asian huomioimista ja korjaamista
Henkilökohtaisten puheluiden soittaminen	Vierailla ja työntekijöillä ei ole mahdollisuutta soittaa henkilökohtaisia puheluita, jolloin he usein käyttävät yksittäisiä toimistoja	Tärkeä	Käytännön määrittely ja siitä tiedottaminen
Faxin käyttäminen	Faxi on sijoitettu henkilökohtaiseen toimistoon	Tärkeä	Käytännön määrittely ja siitä tiedottaminen
Paloturvallisuus: Sammuttimet	Sammuttimien käyttöä ei ole harjoiteltu ja elektroniselle laitteistolle ei ole olemassa hiilidioksiini sammutinta	Tärkeä	Sammuttimien käytön ohjeistaminen tai harjoittelu. Hiilidioksiini sammuttimen hankkiminen. Yläkerran vaahtosammuttimen huolto tulisi huolehtia.
Vieraskäytännön puuttuminen	Neuvotteluhuoneet monesti siivoamatta ja tiedottaminen epäyhdenmukaista.	Tärkeä	Ohjeistus vieraskäytännöille
Lounastuntien aikana toimitiloissa ei välttämättä ole työntekijöitä	Tällä hetkellä on mahdollista, ettei toimistossa ole työntekijöitä lounasaikaan paikalla. Tämä ei ole hyväksi yrityskuvalle ja lisää mahdollisia tietovarkausriskejä.	Tärkeä	Yksinkertainen ohjeistus ovien lukitsemisesta on riittävä tätä varten.
Paloturvallisuus: toimitilojen evakuoiminen	Toimitiloista poistumista ei ole harjoiteltu, eikä toimenpiteitä ole ohjeistettu	Melko tärkeä	Ohjeistuksen laatiminen ja harjoituksen pitäminen
Henkilökunnan reagointi vieraisiin	Ei ole olemassa yhteistä käytäntöä miten vieraisiin suhtaudutaan	Ei tärkeä	Yksinkertaisen menettelyn laatiminen ja siitä tiedottaminen
Asiakastilojen tietoturvallisuus	Asiakkaat kulkevat koko toimiston läpi ja heidän liikkumista ei voida kontrolloida. Neuvottelu huoneisiin näkee sisälle ja kovemmat äänet kuuluvat ulkopuolelle	Ei tärkeä	Tulee huomioida muutettaessa uusiin toimitiloihin
Ensiaputaitoiset henkilöt	Onko yrityksessä riittävä määrä ensiaputaitoisia henkilöitä?	-	Tilanteen tarkastaminen
Vastuualueiden selkeyttäminen	Toimitilojen hoitoon osallistuu kolme erillistä tahoa	-	Toimitilojen ylläpidon vastuullistaminen yhdelle taholle

Taulukon 3 mukaan, vastaajat kokivat tärkeäksi, että neuvotteluhuoneet pidetään siisteinä ja ne siivotaan jokaisen kokouksen jäljiltä. Tällöin varmistutaan, että asiakastiloissa ei ole mitään luottamuksellista tietoa ja näin yritys luo itsestään luotettavan kuvan yhteistyökumppaneille ja asiakkaille. Vastaajien mielestä henkilökunnan tulisi osata reagoida vieraisiin. Erityisesti tarpeellista tämä koetaan olevan silloin, kun asiasta tavallisesti vastaava toimistosihteeri ei ole paikalla. Yrityksessä ei ole ohjeistusta tai toimintamääräystä näiden asioiden toimeenpanosta. Yleistä vieraskäytäntöä ei kuitenkaan nähty tärkeänä asiana yrityksessä. Laajempi vieraista tiedottaminen ei ole vastaajien mukaan oleellista liiketoiminnalle. Yksi vastaajista kommentoi vieraista tiedottamisesta: ”*Kaikkien ei ole tarpeellista tietää kuka vieraileva taho käy yrityksessä*”. Vieraskäytännöille tulisi tehdä selkeä ohjeistus, kokoustilojen käytöstä ja mahdollisesta tiedottamisesta. Ohjeistus tulisi suunnata kutsujille. Henkilökunnalle ei ole tarpeellista tehdä erillistä ohjeistusta vieraita varten, mutta yksinkertainen menettely vieraita kohtaan tulisi olla. Yrityksen henkilökunnan pitäisi olla tietoinen toimistoista, joista he saavat soittaa rauhassa puheluita. Operatiivisen toimitusjohtajan toimistossa olevan faxin käyttöä tulisi valvoa. Myös lounastunnit tulisi huomioida yrityksen toiminnassa paremmin. Tällä hetkellä on mahdollista, ettei toimistolla ole paikalla ketään työntekijöitä toimistoaikoina. Tämä ei ole hyväksi yrityskuvalle ja lisää näin mahdollisia tietovarkausriskejä. Yksinkertainen ohjeistus ovien lukitsemisesta on riittävä tätä varten.

Rakennuksen turvallisuutta ei koettu kovinkaan luotettavaksi, erityisesti päiväaikaan ei voida puhua varsinaisesta pääsynvalvonnasta. Vartiointiliikkeen reagointinopeutta myös epäiltiin. Kuitenkin rakennuksen turvallisuus koettiin riittäväksi liiketoiminnalle.

Toimitilojen turvallisuus käsitti vieraskäytännöt, asiakastilat, paloturvallisuuden ja palvelintilojen turvallisuuden. Vieraiden kulkureittien ja toimitiloissa liikkumisen valvomista ei koettu tärkeäksi. Kokoustilojen ääni- ja näköeristystä ei myös nähty oleelliseksi liiketoiminnan kannalta. Edellämainitut asiat tulisi kuitenkin huomioida uusiin toimitiloihin muutettaessa. Yksi vastaajista huomautti, että yrityksessä ei ole erillistä tilaa soittaa henkilökohtaisia puheluita, jonka takia etenkin työntekijät käyttävät usein yksityisiä toimistoja puheluiden soittamiseen. Faxi on myös sijoitettu operatiivisen toimitusjohtajan toimistoon.

Paloturvallisuutta ei ole huomioitu henkilökunnan koulutuksessa tai tiedottamisessa. Sammuttien käyttöä ja toimitiloista poistumista ei ole harjoiteltu, eikä ohjeistettu, miten tulee toimia jos työpiste pitää jättää palohälytyksen takia. Neljä vastaajaa ei nähnyt asiaa tärkeänä liiketoiminnan kannalta. On kuitenkin tärkeää, että on olemassa ohjeistus, miten tulee toimia tulipalon tai muun kriisitilanteen sattuessa, jossa työpiste joudutaan jättämään. Seuraavat asiat tulisi ainakin huomioida: tuleeko ottaa jotain mukaan, lukita laatikot, toimiston ovet tai työasema. Yksi vastaaja myös epäili, onko yrityksessä riittävä määrä ensiaputaitoisia henkilöitä. Palvelintilojen turvallisuus oli vastaajien mielestä riittävä ja vastuualue oli selkeä. Yksi palosammutin tulisi olla hiilidioksiidi sammutin, jotta sillä voitaisiin sammuttaa tarvittaessa elektronisia laitteistoja.

Vastuuhenkilön määrittelyssä tuli selvästi esille, että usea eri ihminen on osallistunut toimitiloihin liittyviin tehtäviin. Vastuualueet määritettiin toimistovastaavalle, henkilöstöhallinnalle ja ylimmälle johdolle. Suurimmalle osalle vastaajista oli epäselvää, kuka on vastuullinen itse rakennuksen turvallisuudesta. Nykyiset tehtävät tulisi evaluoida ja arvioida, voidaanko kaikki tehtävät vastuuttaa yhdelle henkilölle, jolle tulisi lisäksi määrittää varahenkilö.

6.3 Tietojärjestelmien suojaus

Taulukko 4 Tietojärjestelmien suojauksen kehityskohteet

Kehityskohde	Ongelman kuvaus	Prioriteetti	Toimenpiteet
Tiedon suojaaminen asiattomilta käyttäjiltä	Liiketoimintakriittistä tietoa ei ole suojattu kryptauksella. Kaikilla ei ole käytössä lukittavaa laatikostoa	Erittäin tärkeä	Toimenpiteiden kartoittaminen ja havainnollistaminen
Tunnus- ja salasanakäytäntö	Käytössä palveluita tai järjestelmiä, joita hallinnoidaan yhdellä salasanalla.	Erittäin tärkeä	Arvioidaan, onko mahdollista siirtyä käyttämään käyttäjäkohtaisilla tunnuksilla
Tiedon luokittelu luottamuksellisuuden mukaan	Ei systemaattista tiedonluokittelua	Tärkeä	Projektiryhmän kokoaminen ja luokiteltavan tiedon tunnistaminen
Työntekijän sähköpostin lukeminen poikkeus tilanteessa	Työntekijöiden kanssa on sovittu työnantajan oikeudesta lukea työntekijän työsähköposti tarvittaessa.	Tärkeä	Käytännön määrittäminen, dokumentointi ja tiedottaminen
Toimisto-ohjelmistojen yhteensopivuus	Useita erillisiä ohjelmistoja tai eri ohjelmaversioita käytössä	Tärkeä	Ympäristön yhdenmukaistamisesta koituvien kulujen kartoittaminen
Kannettavien suojaaminen	Kannettavien laitteiden suojaaminen kryptauksella satunnaista	Tärkeä	Kannettavien ja mahdollisesti puhelimien kryptaus ja käyttäjien ohjeistaminen
Siirrettävien massamuistien (USB-tikut) käytön ohjeistaminen	Nykyinen käyttö perustuu oletukseen henkilökunnan tietoturvatietoisuudesta. Tiedon siirtäminen on kontrolloimatonta.	Melko tärkeä	Käyttöpolitiikan tai ohjeistuksen laatiminen

Taulukon 4 mukaan, tiedonluokittelua tiedon luottamuksellisuuden mukaan ei ole toteutettu systemaattisesti yrityksessä. Yksittäiset tahot käyttävät tiedonluokittelua tiedon luottamuksellisuuden mukaan, mutta sitä ei ole toteutettu järjestelmällisesti. Seitsemän vastaajista koki, että tiedonluokittelu ei toteudu yrityksessä. Kaikkien vastaajien mielestä tiedonluokittelua ei huomioida päivittäisessä liiketoiminnassa. Kahdeksan vastaajista näki tiedonluokittelun tärkeäksi. Vastuullisen tahon nimeäminen oli kuitenkin epäselvää vastaajille. Kolme vastaajista nimesi johdon vastuulliseksi tahoksi ja yksi vastaajista ehdotti projektiryhmän kokoamista asian toteuttamiseksi. Tiedon suojaaminen yrityksessä on usean tahon vastuulla, joka näkyikin vastauksissa valittujen vastuualueiden suurena hajontana. Kaiken kaikkiaan vastaajat olivat sitä mieltä, että tieto on suojattu asiattomalta käytöltä. Seitsemän vastaaja koki, että liiketoiminta kriittinen

tieto tulisi suojata kryptaamalla. Tämän asian läpikäyminen ryhmässä on järkevää, jotta kaikki ymmärtävät, minkälaisista toimenpiteistä on kysymys tiedon kryptaamisessa.

Fyysisten laitteiden tai dokumentaatioiden suojaamiseksi tulisi kaikilla olla lukolliset kaapit. Tämä oli pääasiassa toteutettu yrityksessä hyvin. Yksi vastaaja tarkensi asiaa siten, että jokaisen tulisi ottaa asiasta vastuu, jolla on tärkeää tietoa hallussa. Jokaisen työntekijän tulisi kuitenkin osata huomioida tietoturva toiminnassaan, joten ohjeistaminen on ainoa keino minimoida riski tietojen menettämisestä.

Salasana- ja tunnuskäytännöissä tulivat ilmi seuraavat haavoittuvuudet. Tuotantotiloissa on tiettyihin järjestelmiin käytössä ainoastaa yksi yhteinen käyttäjätunnus ja salasana. Myös useiden palvelimien ja informaatiopalveluiden käyttöön on henkilöstöllä yhteistunnuksia. Henkilöstön yhteisesti käytettävissä olevaan multimedia-työasemaan on pääsy yhteistunnuksella - tosin tämä luo ainoastaan uhan kyseisellä työasemalla säilytettävälle tiedolle. Tietohallinnon tulisi laatia ohjeet ja henkilöstöhallinnan ja/tai esimiesten tulisi huolehtia, että työntekijät lukevat ohjeet läpi ja ymmärtävät asiassa yrityksen ja työntekijän vastuun.

Työnantajan oikeudet sähköpostin lukemiseen poikkeustilanteissa olivat seitsemälle vastaajalle epäselvät ja vastaajat kokivat, että asiasta ei ole erikseen sovittu tai keskusteltu. Kaksi vastaajista koki asian olevan erittäin selkeästi hoidettu. Vastuussa oleva taho oli kuitenkin epäselvä. Tietohallinnon prosessit, kuten käyttöoikeuksien hallinta, olivat epäselviä vastaajille. Viisi vastaajista koki, että tietohallinto on vastuullinen työntekijöiden pääsystä vain ja ainoastaan työtehtävien suorittamiseen vaadittavaan tietoon. Tietohallinto ei kuitenkaan voi olla tietoinen, mihin tietoon työntekijöillä on oltava pääsy. Tietohallinto on dokumentoinut prosessit, mutta niistä ei ole tiedotettu riittävästi.

Toimisto-ohjelmistojen yhteensopivuus jakoi vastaajat kahtia, neljän mielestä ohjelmistot olivat riittävän yhteensopiva ja viiden mielestä eivät. Yrityksessä on käytössä MS-Office (Microsoft Office) 2003, 2007 ja 2010 versiot ja Open Office 3.x versio ja lisäksi MAC OS:lle tehty MS-Office. Viisi vastaajaa on törmännyt aika ajoin yhteensopimattomuusongelmiin. Kaksi vastaajista ei kuitenkaan kokenut asiaa liiketoiminnallisesti tärkeäksi. MS-Office koettiin myös välttämättömäksi työskennellessä asiakasrajapinnassa. Toimistoohjelmistojen yhteensopivuus koettiin olevan tietohallinnon vastuulla. Olettaen, että tiedon eheys halutaan säilyttää, niin useamman toimistoohjelmiston käyttö todennäköisesti rikkoo tiedon eheyden.

Siirrettävien massamuistien käyttämiseen ei ole olemassa erikseen määritettyä prosessia, ja massamuisteja ei ole suojattu kryptaamalla. Yksikään vastaajista ei kokenut kryptaamista vaihtoehtona, mutta ohjeistaminen massamuistien käytöstä koettiin tärkeäksi. Nyrkkisääntönä osa vastaajista piti, että siirrettäville massamuisteille ei tulisi milloinkaan tallentaa mitään luottamuksellista tai liiketoiminnalle oleellista tietoa. Yrityksen kannettavia tietokoneita ja puhelimia ei myöskään pääsääntöisesti ole suojattu kryptaamalla.

6.4 Henkilöstön tietoisuus ja toimintatavat

Taulukko 5 Henkilöstön tietoisuus ja toimintatavat

Kehityskohde	Ongelman kuvaus	Prioriteetti	Toimenpiteet
Tiedon luokittelu luottamuksellisuuden mukaan	Henkilökunta ja osa esimiehistä ei ole tällä hetkellä täysin tietoinen, mikä on luottamuksellista tietoa ja kuinka sitä tulisi käsitellä	Erittäin tärkeä	Tiedon luokittelun aloittaminen ja sen käytön ohjeistaminen
Käyttäjiin/palvelujen käyttämiseen ja palveluihin kohdistuvien tietoturvauhkien kartoitus	Käyttäjät eivät todennäköisesti olisi kykeneviä tunnistamaan tietoturva uhkaa tällä hetkellä	Erittäin tärkeä	Uhkien tunnistaminen ja henkilökunnan ohjeistaminen uhkista.
Ohjeistuksien jalkauttaminen henkilöstölle	Henkilöstö ei ole lukenut läpi tietoturvapolitiikkaa, yrityksen-toimitila politiikkaa (company policy) ja tietohallinnon prosessikuvauksia.	Erittäin tärkeä	Politiikkojen läpikäynti ja ajantasaistaminen. Esitellään politiikat henkilökunnalle ja varmistetaan, että kaikki ovat ymmärtäneet lukemansa.
Käyttö oikeuksien hallinta ja tiedostaminen	Esimiehet eivät ole tietoisia, mihin järjestelmiin heidän alaisillaan on pääsy.	Erittäin tärkeä	Toimivan käytännön laatiminen (Pääsynvalvonta matriisi)
Yrityksen omaisuuden hallinnan tehostaminen	Ei ole olemassa sopimusta, jossa on listattu työntekijän hallussa oleva yrityksen omaisuus. (laitteet, tieto).	Erittäin tärkeä	Sopimuksen laatiminen, joka allekirjoitetaan työsuhteen alkaessa ja jota päivitetään.
Jatkuvuussuunnitelma avainhenkilöille	Toiminta ei keskeydy yksittäisen henkilön äkkinäisen irtisanoutumisen tai muun pitkäaikaisen poissaolon takia	Erittäin tärkeä	Avainhenkilöiden kartoittaminen ja mahdollisten varautumissuunnitelmien laatiminen
Työntekijän irtisanominen ristiriitatilanteessa	1 vastaaja näki, että asia ei ole kunnossa 4 ei ollut tietoisia ja 1 koki osittain olevan ja osittain ei.	Erittäin tärkeä	Tarkistetaan onko prosessi olemassa vai ei ja selvitetään tämä johdolle.
Etätyön ohjeistaminen	Etätyötä ei ole ohjeistettu	Erittäin tärkeä	Tarvittavan ohjeen laatiminen
Rekrytointi ohjeistus	Ei ole olemassa yhdenmukaista rekrytointi käytäntöä.	Tärkeä	Vastuualueiden selkeyttäminen ja rekrytoinnin ohjeistaminen.
Sähköpostipolitiikka	Ei yhtenäistä sähköpostipolitiikkaa. Ulkomaan toimisto käyttää henk.koht sähköpostiosoitteita.	Tärkeä	Evaluoida nykyinen politiikka ja sitoa se osaksi tietoturvapolitiikkaan.
Internet-politiikka	Työntekijät eivät ole tietoisia Internet politiikasta ja siihen ei välttämättä ole sisällytetty johdon näkemyksiä	Tärkeä	Evaluoida nykyinen politiikka ja sitoa se osaksi tietoturvapolitiikkaan.
Työasemien lukitseminen	Työasemia ei aina lukita työntekijöiden poistuessa työpisteeltä. Avoin työaseman on portti yrityksen verkkoon ja järjestelmiin	Tärkeä	On ohjeistettu, mutta ei valvota
Varmuuskopioinnin ohjeistaminen	Varmuuskopioinnin ohjeistusta ei ole dokumentoitu	Tärkeä	Toimintamallin evaluointi ja dokumentointi

Taulukon 5 mukaan, vastaajat eivät kokeneet henkilökunnan tiedostavan yrityksen, eikä työntentekijän vastuuta luottamuksellisuuden ja tietoturvallisuuden suhteen. Osa esimiehistä koki, että heidän työntekijänsä eivät oikeasti ole tietoisia, mitä he saavat kertoa eteenpäin. Yksi vastaajista totesi myös, että heidän yksiköllään ei ole mitään tärkeätä tietoa. Toisaalta eräs vastaaja kommentoi aihetta seuraavasti ”*Omasta toiminnasta voi sanoa, että luottamuksellista tietoa ei mene ulos, mutta muista toimijoista ei ole tietoa. Omasta tiimistä on varmuus, että kaikilla on terve ymmärrys luottamuksellisesta tiedosta.*”. Jokainen vastaaja koki tiedon luottamuksellisuuden ymmärtämisen tärkeänä liiketoiminnan kannalta. Vastuulliseksi tahoksi koettiin ylin johto, henkilöstöhallinto ja esimiehet. Näiden mielipiteiden pohjalta voidaan olettaa, että henkilökunnan tietoisuutta tietoturvallisuudesta tulisi kehittää. Toimiva malli voisi olla tiedonluokittelun aloittaminen yrityksessä. Tällöin tiedon luottamuksellisuuden mukaan voidaan ohjeistaa, kuinka luottamuksellista tietoa tulisi ja saa käsitellä. Yksi vastaaja koki luottamuksellisen tiedon käsittelyn nykyisen käytännön yrityksessä seuraavasti *”Uskon, että henkilöt jotka ovat aktiivisesti liiketoiminnassa mukana ymmärtävät asioista tämän puolen, mutta ei varmasti koske kaikkia. Ja ei ole jokapäiväinen käytäntö luokitella tietoa. Tulisi tarkastaa projektien yhteydessä ymmärtääkö henkilö tämän luottamuksellisuuden merkityksen.”*

Kaikkien vastaajien mielestä tietohallinto on vastuussa tietoturvahaavoittuvuuksista yrityksessä. Tietoturva haavoittuvuuksien tunnistamisen vaikeudesta, yhdellä vastaajalla oli hyvä huomio ”*Kaikilla ei varmasti tietoa, että mikä on vakava tietoturvauhka ja kuinka tunnistetaan tietoturvahyökkäys tai todellinen uhka.*”. Tämän huomion perusteella päättelin, että tulisi kartoittaa vakavat uhat, jotka voivat kohdistua suoranaisesti käyttäjiin. Käyttäjiä tulisi informoida näistä uhista ja ohjeistaa, miten uhan havaittua tulee toimia.

Vastaajien mielestä yrityksessä ei ole huolehdittu, siitä että työntekijät olisivat lukeneet yrityksen tietoturvapolitiikkaa, yrityksentoimitilapolitiikka (company policy) ja tietohallinnon prosessikuvauksia. Jokainen työntekijä on allekirjoittanut vaitiolosopimuksen, mutta ei ole varmistettu, että onko työntekijä on ymmärtänyt vaitiolosopimuksen merkityksen. Tietohallinto on dokumentoinut prosessinsa, mutta niistä tiedottamisessa on epäonnistuttu. Esimerkiksi vain viisi vastaaja oli tietoinen, että yrityksessä on olemassa selkeä prosessi uuden työntekijöiden oikeuksien luomiseksi. Jokainen vastaaja koki tämän kuitenkin tärkeäksi. Vastuulliseksi tahoksi viestinnän varmistamiseksi koettiin tietohallinto, henkilöstöhallinto ja esimiehet. Yksi vastaaja kommentoi vastuualueisiin seuraavasti, ”*Tietohallinnon tulisi laatia ohjeet ja henkilöstöhallinnon tai esimiesten tulisi huolehtia, että työntekijät lukevat ohjeet läpi ja ymmärtävät yrityksen ja työntekijän vastuun.”*

Työntekijöiden oikeuksien hallinnasta kuusi vastaaja koki, että esimiehet eivät ole tietoisia, mihin tietojärjestelmiin heidän alaisillansa on pääsyoikeudet. Tietohallinnosta ei yksikään kolmesta vastaajasta kokenut asian olevan kunnossa. Kahdeksan vastaajaa näki tämän olevan esimiesten vastuulla. Kyselyn aikana tuli esille, että ylinjohto välillä sivuuttaa työntekijöiden suorat esimiehet oikeuksien hallinnassa, ja näin esimiehet eivät

välttämättä saa tietoa muutoksista. Yksi vastaaja totesi asiasta *”On tärkeätä, että käyttöoikeuksien hallinta toteutetaan pelkästään esimiesten toimesta. Tieto tämän hetkisistä käyttöoikeuksista ei ole tarpeellinen olla jatkuvasti saatavilla”* Yllättävää oli, että viisi vastaajaa näki, että esimiehet eivät ole tietoisia siitä, että mihin järjestelmiin uusilla työntekijöillä on oikeudet. Ainoastaan kolme vastaajaa koki, että esimiehet ovat tietoisia uusien työntekijöiden oikeuksista. Myös poistuvien työntekijöiden oikeuksien hallinnan koki seitsemän vastaajaa puuttelliseksi. Tiedonsuojaaminen työsuhteen loppuessa koettiin olevan hyvin hallinnassa. Kuitenkin nähtiin mahdolliseksi, että lähtevä työntekijä voisi mahdollisesti aiheuttaa vahinkoa yrityksen tiedoille tai järjestelmille. Vastaajat kokivat edellä mainittujen asioiden olevan tietohallinnon, henkilöstöhallinnon ja esimiesten vastuulla. Käyttöoikeuksiin liittyvät prosessit tulisi dokumentoida tietohallinnon, henkilöstöhallinnon ja esimiesten kanssa yhteistyössä. Lopputuloksena olisi pääsynvalvonta matriisi, josta esimiehet voivat tarkastaa voimassa olevat pääsyoikeudet.

Vastaajilta kysyttiin, onko olemassa sopimus yrityksen omaisuuden palauttamisesta työsuhteen loppuessa. Kolme vastaajista koki, että ei ole olemassa mitään sopimusta, jossa työntekijä olisi kuitannut vastaanottaneensa yrityksen omaisuutta ja sitoutuisi luovuttamaan yrityksen työntekijälle käyttöön luovutetut laitteet ja palauttamaan tiedot takaisin yritykselle työsuhteen loppuessa. Neljä vastaajista ei ollut tietoisia, onko tälläistä sopimusta olemassa. Jokainen vastaaja näki sopimuksen omaisuuden luovuttamisesta tärkeänä ja vastuullisena tahona henkilöstöhallinnon. Esimiesten tietoisuus työntekijöiden hallussa olevasta omaisuudesta tulkittiin erittäin ristiriitaisesti. Yksikään vastausvaihtoehto ei saanut kahta ääntä enempää, kaikki vastaajat kokivat tämän kuitenkin tärkeänä.

Ristiriitatilanteissa tapahtuvat irtisanomiset koettiin olevan pääosin hallinnassa, varsinkin henkilöstö- ja tietohallinnan osalta. Kuitenkin vastaajille oli epäselvää, onko olemassa tietty prosessi ongelmatilanteen hoitamiseksi. Jos irtisanomisprosessi ongelmatilanteessa perustuu yhden henkilön hallussa olevaan tietoon, ei voida puhua hallussa olevasta prosessista. Tämä mahdollistaa väärinkäsityksiä ongelmatilanteessa ja luo näin monia riskejä. Jatkuvuussuunnitelmaa ei koettu olevan olemassa, jos avainhenkilöt irtisanoutuvat tai joutuvat jostain toisesta syystä olemaan pitkään poissa liiketoiminnasta. Kolme vastaaja näki, että heidän osastollaan on jatkuvuussuunnitelma huomioitu. Jokainen vastaaja koki tämän olevan tärkeää liiketoiminnalle.

Uusien työntekijöiden rekrytoinnissa ei aina voida huomioida työntekijöiden osaamista yrityksen tietojärjestelmien käytössä. Pääasiallisena syynä tähän nähtiin liiketoiminnan nopea kasvu ja heikko ennustettavuus. Yksi syy oli myös henkilökunnan vaihtuvuus. Rekrytointien yhteydessä työnhakijoiden tietojen oikeellisuus tarkistetaan työtehtävän luottamuksellisuuden ja tärkeyden mukaan. Kolme vastaajaa viittasikin talousjohtajan rekrytoinnissa tapahtuneeseen tietojen oikeellisuuden tarkastamiseen, joka oli tehty erittäin perusteellisesti. Tämä työtehtävän luottamuksellisuuden mukaan tehtävä tietojen oikeellisuuden tarkistus on varmasti oikea tapa hoitaa, koska neljä vastaajaa ei kokenut hakijoiden taustojen selvitystä tärkeänä liiketoiminnan kannalta. Kaiken kaikkiaan vastauksissa oli havaitta-

vissa, että kaikille ei ole selvää, mikä on esimiehen ja henkilöstöhallinnon vastuu rekrytoinnissa. Rekrytointiprosessi voisikin olla järkevää dokumentoida.

Yrityksessä ei koettu olevan Internetin käyttöpolitiikka. Seitsemän vastaaja näki tämän tärkeäksi liiketoiminnan kannalta. Asiasta annettiin seuraavia mielipiteitä ”*Kieltäisin Facebookin, joka on ajanhukkaa. Pääasiassa liiketoiminta on B2B myyntiä, Facebook ei tuo riittävää lisäarvoa, jotta siihen kannattaisi käyttää aikaa tai energiaa. Ei varmasti ole prioriteetti yksi tehtävissä asioissa.*”, ”*Osa työntekijöistä käyttää paljon aikaa päivittäin Facebookissa ja oletettavasti tämä ei kuulu heidän työnkuvaan*”. Facebookin käytölle voitaisiin luoda käyttöpolitiikka tai toimintamalli. Henkilöt, ketkä sitä käyttävät työssään tulisi määrittää ja tästä tulisi tiedottaa. Työtehtävät ja tavoitteetkin olisi järkevää dokumentoida - miksi, kenelle, mitä palvelun käyttämisellä saavutetaan. Ennen yksittäisten Internetpalvelujen kieltämistä olisi hyvä harkita kiellon seuraamuksia - kiellot saattavat herättää negatiivisen reaktion henkilökunnassa. On myös ihmisluonteelle ominaista, että kieltoja kierretään, joten seuraamukset kiellon rikkomisesta tulisi määrittää. Facebookin käytöstä koituvia haittoja ja hyötyjä olisi varmasti syytä evaluoida. Yksikään vastaaja ei huomauttanut muista sosiaalisen median tai verkkoviestintä ohjelmistoista kuten Twitter, Skype, Messenger ja Gmail. Sähköpostipolitiikan koki kuusi vastaajaa puuttuvan yrityksestä. Yksi vastaajista huomautti, että ulkomailla ja Suomessa ei ole yhtenäistä shköpostikäytäntöä. *”Sähköpostin käytössä on poikkeavaisuuksia ulkomaan toimipiste käyttää työsähköpostina henkilökohtaisia GMAIL-sähköpostiosoitteita. Suomessa kaikki käyttävät vain ja ainoastaan yrityksen virallista sähköpostia. Yrityksessä tulisi olla yhtenäinen linja sähköpostin käyttöön.*”

Kuusi vastaajaa koki, että työntekijöitä on ohjeistettu lukitsemaan työasemansa poistuessaan työpisteeltänsä ja kahdeksan vastaaja koki asian tärkeäksi. Kahdeksan vastaajaa näki tämän olevan tietohallinnon vastuulla, vaikka tietohallinnolla ei ole mahdollisuutta valvoa ohjeen noudattamista. Yhdeksän vastaajaa näki, että työntekijän henkilökohtaiset tiedot on suojattu riittävät hyvin ulkopuoliselta taholta. Varmuuskopiointia ei ole ohjeistettu henkilökunnalle paitsi suullisesti. Pitempään talossa olleet työntekijät olivat saaneet ohjeet varmuuskopioiden ottamisesta, mutta eivät palauttamisesta. Uusia työntekijöitä ei ollut ohjeistettu laisinkaan. Varmuuskopioinnista tulisi olla selkeä kirjallinen ohjeistus henkilökunnalle. Seitsemän vastaaja näki tärkeäksi, että varmuuskopiot olisivat keskitetysti hallittu. Varmuuskopionti nähtiin olevan tietohallinnon vastuulla. Kolme vastaaja koki, että työntekijät kykenevät asentamaan omia sovelluksia yrityksen työasemille.

6.5 Liiketoiminnan kehittämistarpeet tietoturvallisuuden toteuttamiseksi

Taulukko 6 Liiketoiminnan kehittämistarpeet tietoturvallisuuden toteuttamiseksi

Kehityskohde	Ongelman kuvaus	Prioriteetti	Toimenpiteet
Tiedonjakaminen	Liiketoiminta ja siihen liittyvä tietämys on yhden henkilön varassa. Onko tietoa edes mahdollista jakaa?	-	Tulee arvioida ja päättää ryhmässä
Yhteisen viestintämallin luominen	Yrityksestä puuttuu selkeä yhtenäinen viestintä käytäntö ja ohjeistus asioista, joista tulee informoida.	-	Sopia viestintämenetelmästä, tiedottaa, varmistaa viestin perillemeno ja seurata
Esimiesten koulutus	Esimiehiä ja johtoa ei ole ohjeistettu ja koulutettu tehtäviinsä. Yleisesti ottaen ei ole oppaita tai ohjeistoja olemassa kuinka toimia.	-	Osaamisalueiden kartoittaminen. Päättää mahdollisista koulutuksista ja tarvittavista ohjeistuksista. Työnkuvien laadinta.
Työntekijöiden koulutus	Työntekijöiden koulutuksen on oltava puutteellista, jos johdonkin koulutus on. Esimerkiksi varmuuskopiointia ei ole koulutettu tai ohjeistettu. Tuotannossa on ilmennyt tietämättömyyteen liittyviä ongelmia.	-	Tulee arvioida ja päättää ryhmässä
Työntekijöiden vaihtuvuus	Jatkuva perehdytys vie kaikkien aikaa ja koulutuksen toistamisen tarve nousee. Työntekijän vaihtuessa on opetettava uudestaan esim. yrityksen- toimintatavat, kulttuuri, politiikat, tietojärjestelmien käyttö, työskentelytavat…	-	Tulee arvioida ja päättää ryhmässä
Tietoturvallisuuden sitominen osaksi johtamista	Tietoturvallisuutta ei tulisi kehittää erillisenä osa-alueena vaan sen huomioiminen tulisi olla osa päivittäistä johtamista.	-	Tulee arvioida ja päättää ryhmässä

Taulukossa 6 ovat liiketoiminnan kehittämistarpeet tietoturvallisuuden toteuttamiseksi, jotka nousivat useiden vastaajien kanssa esille epäsuorasti. Ongelmat voidaan tiivistää kahteen asiaan tiedonjakamiseen ja henkilöstön koulutukseen. Liiketoiminnan johdolta ei ole aina saatavilla selkeätä tietoa liiketoiminnan tavoitteista - tämä luo epävarmuutta. Ylimmän johdon työnkuvia ei ole laadittu yrityksessä yhdenmukaisesti ja keskitetysti. Ylemmän johdon työnkuvat ovat kehittyneet työssä liiketoiminnan tarpeita vastaavaksi. Ylempi johto on ensisijaisesti itse vastuussa työnkuviensa kehittämisestä ja niihin mahdollisesti liittyvien mitattavissa olevien tavoitteiden asettamisesta. Henkilöstön huomattavan suuri vaihtuvuus on myös haasteellista sisäisen koulutuksen kannalta - koulutuksia tarvitaan aina henkilöiden vaihtuessa. Henkilöstön perehdyttämiseen ja kouluttamiseen ei ole ollut riittävästi aikaa ja resursseja yrityksen kasvun kiihtyessä. Tämä

heikentää toiminnan tehokkuutta ja lisää epätietoisuutta yrityksen toimintamalleista henkilökunnan keskuudessa.

Yrityksen johtamista tulisi hallita keskitetymmin - tulisi pyrkiä eroon organisaatiokulttuurista, jossa yrityksen avainhenkilöillä ei ole saatavilla luotettavaa tietoa liiketoiminnan nykyisestä tilanteesta. Yrityksen sisäistä viestintää olisi kehitettävä, jotta eri tahot eivät kehittäisi ja ylläpitäisi yrityksessä päällekkäisiä prosesseja.

Henkilökohtaisesti näen, että edellä mainitut ongelmat ovat muodostuneet ajan myötä yrityksen kasvettua kymmenen hengen yrityksestä kuudenkymmenen hengen yritykseksi. Erilaisia toimintaprosesseja on kehitetty tarpeen mukaan lukuisten eri henkilöiden toimesta ilman niiden keskitettyä hallintaa. Tämän vuoksi yrityksessä on paljon lähes valmiita toimintaprosesseja, mutta tieto niiden hallinnasta ja toiminnallisuudesta ei ole välittynyt henkilökunnalle. Vastaajat kommentoivat seuraavasti *”Meitä ei ole ohjeistettu tiedon suojaamiseen tai käsittelyyn”, ”Yleisesti ottaen ei ole olemassa ohjeistuksia tai toimintamalleja”.* On huomioitava, että kaikkea ei tule dokumentoida. Ohjeistuksien dokumentointi tulisi huomioida ohjeiden tarpeellisuuden ja käytettävyyden mukaan. Yksi vastaaja kuvasi dokumentoinnin hallitsemista ja tarpeellisuutta seuraavasti ”*Kaikkea ei voi ja ei kannata laittaa paperille, koska silloin itse ydinasia hukkuu.*”, ”*Liiketoiminnassa on lukuisia kirjoittamattomia tapoja, joiden kirjoittaminen ja niistä tiedottaminen ei ole organisaatiotasolla tarpeellista. Esimerkiksi meille on pukeutumiskoodi oleellinen, mutta sen tietäminen ei ole tärkeää kaikille.*”

6.6 Kyselyn toimivuus

Kyselyn lopuksi kysyin kaikilta vastaajilta mielipidettä tietoturvariskikyselyn toimivuudesta. Ensimmäiseä kysymyksenä kysyin, että oliko läsnäolostani kyselylomakkeen täytön aikana hyötyä. Kaikki vastaajat kokivat tutkijan läsnäolon hyödylliseksi. Henkilökohtainen tuki kyselylomakkeen täyttämisessä koettiin motivoivana (”yksin kyselyyn vastatessa olisi turhautunut”), asiasta samalla yleisemmin keskustelua hyvänä ja esimerkkien antamista väittämiin tarpeellisena. Kyselylomakkeessa vaikeina pidetyt väittämät vaihtelivat huomattavasti henkilöiden toimenkuvan mukaan. Seuraavaksi kysyin osallistujilta kyselyn hyödyllisyydestä yritykselle. Kaikki vastaajat kokivat kyselyn hyödylliseksi yritykselle. Muutama vastaaja korosti kuitenkin, että vasta jatkotoimenpiteet määrittävät kyselyn todellisen hyödyllisyyden. Kaikki vastaajat näkivät jatkotoimenpiteet suotaviksi.

Kyselyn pituudesta kysyttäessä suurin osa vastaajista ei kokenut kyselyä liian pitkänä. Kaksi vastaaja koki kyselyn hieman liian pitkäksi ja itseään toistavaksi. Vastaajat kommentoivat pituuteen: ”*Ei se ainakaan pidempi olisi tarvinnut olla*”, ”*Yksin täyttäessä en kyllä olisi täyttänyt näin huolellisesti*”. Näiden kommenttien perusteella voidaan olettaa, että yksin täyttäessä kysely olisi todennäköisesti ollut liian pitkä ja työläs vastaajille. Vastaajat kokivat väittämien määritykset selkeiksi. Keskimäärin vastaajat kokivat johdon tietoisuus-osa-alueen kaikista haastavimmaksi. Kartoitettaes-

sa kyselyn kattavuutta osa-alueiden suhteen vastaajien mukaan kyselystä ei jäänyt käsittelemättä tärkeitä osa-alueita. Suurin osa vastaajista ei ollut perehtynyt tietoturvallisuuteen ja sen osa-alueihin aikaisemmin.

Vastaajat kokivat, että kysely oli ehdottomasti parempi tehdä kahden kesken, koska tällöin on mahdollisuus keskustelulle ilman, että keskustelu lähtisi ”rönsyilemään”. Vastaajat esittivät seuraavia syitä, miksi ryhmään verraten kahdestaan kyselylomakkeen täyttäminen ja keskustelu oli parempi vaihtoehto: ”*Näihin aihealueisiin, jokaisella on oma näkemyksensä, jonka takia tätä ei oltaisi voitu käsitellä ryhmässä*”, ”*Kahden kesken asioista voi keskustella objektiivisesti, osa ihmisistä varmasti kokisi keskustelun omista aihealueistaan henkilökohtaisena*”, ”*Tulisi liikaa keskustelua ryhmässä, fokus pysyy paremmin kaksistaan tehtynä*”. ”*Kahdenkesken on helpompi saada rehellisiä vastauksia.*”. Suurin osa vastaajista oli kuitenkin sitä mieltä, että yhteenveto tulisi tehdä jälkeenpäin ja nimenomaan ryhmässä.

Kysymyslistojen laatimisessa seuraavat kohdat olisi voitu tehdä toimivimmiksi. Kyselyyn oli jäänyt kysymysten tarkistuksesta huolimatta muutama väite, jotka sisälsivät yhden väittämän sijaan kaksi väittämää. Tällöin vastaus ei ole yksiselitteinen. Tietyt väittämät, jotka sisälsivät viittaukseen yrityksen koko henkilökuntaan (”everybody are aware”) olisi ollut parempi muotoilla muotoon ”you are aware...”. Vastaajan on aina helpompi vastata vain omasta puolestaan kuin kaikkien puolesta. Näin vastaukset olisivat voineet tarjota täsmällisempää tietoa. Vastuualuekysymyksen tarkoituksena oli löytää väittämissä esitetyille prosesseille selvät omistajat – ja vastaukseksi hyväksyttiin vain yhden vastuuhenkilön määrittäminen. Kysymyksen vastaus olisi voinut kuitenkin toimia paremmin monivalintana, sillä yrityksessä monet prosessit ovat useiden eri tahojen vastuulla. Vastuualueissa myös ylimmän johdon vastuun määrittely oli haastavaa. Yksi vastaajista kiteytti ongelman hyvin: *”Vastuualueiden määrittely osio on haasteellinen. Koska kaikki on tai kaiken tulisi olla lähtöisin ylimmästä johdosta, mutta joku toinen vastaa toteutuksesta.”*

7 YHTEENVETO

Tutkimusaiheen valinta oli onnistunut ja tutkimus koettiin case-yrityksessä liiketoiminnan kannalta hyödylliseksi. Tutkimuksen tuloksia on tarkoitus hyödyntää yrityksen tietoturvan kehittämisessä. Case-yrityksen tietoriski-analyysissani nousi yrityksen toiminnasta esiin neljä keskeistä ongelma-aluetta. 1) suurin osa yrityksen toimintaprosesseista perustuu olettamukseen, että kaikki yrityksen työntekijät toimivat loogisesti ja ymmärtävät tietoturvan päivittäisessä työssään, 2) puutteellisen viestinnän takia tieto ei välity tietoturvallisuuteen liittyvien prosessien kehittäjiltä käyttäjille - viestin perillemenoa ei varmisteta, 3) toimintaprosessien dokumentointi on puutteellista ja niiden päivittäminen ei ole järjestelmällistä ja 4) henkilökunnan kouluttaminen on riittämätöntä laajojen vastuualueiden hoitamiseen.

Tutkimus toi esille useita tietoturvallisuuden kehityskohteita ja avasi yrityksessä keskustelun tietoturvallisuuden kehittämisestä. Se lisäsi yrityksessä tietoturvatietoisuutta. Tutkimustuloksiin perustuen yrityksessä olisi hyvä suunnitella tulevat tietoturvallisuuden kehitystarpeet ja arvioida tarvittavien resurssien määrää kehitystavoitteiden saavuttamiseksi. Tutkimus osoitti, että yrityksen johdolla ja avainhenkilöillä on yhdenmukainen mielipide tietoturvallisuuden tärkeydestä ja siitä, että se tulisi huomioida liiketoiminnassa.

Tietoturvan kehittämisprojektiryhmän luomisessa on tärkeää, että kaikki liiketoiminnan sisäiset sidosryhmät ovat edustettuina. Case-tutkimuksessani oli mielenkiintoista huomata vastaajien hyvin erilainen lähestymistapa kyselyyn. Kaikki kyselylomakkeeseen vastanneet täyttivät saman kyselyn, ja kävin kysymykset henkilökohtaisesti heidän kanssaan läpi. Vastanneiden henkilöiden ammatilliset, koulutukselliset ja persoonalliset erot tulivat keskustelutilanteessa todella selvästi esille. Näkökulmat eri tietoturvan osa-alueisiin poikkesivat välillä jyrkästi toisistaan. Koen eri sidosryhmien näkökulmien huomioimisen ja osallistuttamisen tietoturvakehitykseen tutkimuksessani arvokkaaksi – ja samalla henkilökohtaisesti opettavaiseksi. Pitäisin eri sidosryhmistä koostuvan projektiryhmän kokoamista järkevänä lähestymistapana myös muun tyyppisissä yrityksen sisäisissä kehitysprojekteissa.

Pk-yrityksessä on huomioitava tarkkaan käytettävissä olevat resurssit ja sisäinen tietoturva- ja riskienhallintaosaaminen. Tarkistuslistojen käytössä ei tarvita kovinkaan syvällistä osaamista, mutta perusymmärrys tietoturvasta on oltava, jos tarkistuslistoja halutaan käyttää tehokkaasti. Tarkistuslistat ovat tehokas tapa tehdä yleiskartoitus tietoturvan kokonaistilasta yrityksessä. Jos tutkittava kohde on tarkkaan rajattu, niin tarkistuslistojen käyttäminen tietoturvariskien kartoitukseen ei ole suositeltavaa. Tarkistuslistat eivät sovellu myöskään erityisen hyvin teknisten kohteiden tietoturvariskien analysointiin, vaan ne vaativat syvällisempää lähestymistapaa. Tietoturvariskianalyysimenetelmä on valittava aina tapauskohtaisesti ja sen valinta on pystyttävä perustelemaan.

Usein tietoturvan kehittäminen ja hallinta on pk-yrityksissä satunnaista, ja järjestelmällisten prosessien sijaan luotetaan asioiden hoitamiseen tarpeiden realisoituessa. Prosessien puutteellisuuden ja liiketoiminnan mahdollisten suurien muutosten takia tietoriskienhallinta on järkevää aloittaa pk-yrityksessä osana liiketoiminnan johtamista. Tällöin tietoturvallisuus huomioidaan yrityksen päivittäisessä toiminnassa, ja se tukee yrityksen muita turvallisuusalueita. Tietoturvallisuuden huomioiminen ja järjestelmällinen kehittäminen päivittäisessä liiketoiminnassa estää lukuisten erillisten tietoturvaprosessien muodostumisen yritykseen. Tämä tuo yritykselle kustannussäästöjä tehokkuuden lisääntymisen myötä. Tietoturvallisuuden huomioiminen pienentää epätoivottujen tapahtumien todennäköisyyttä ja parantaa näin yrityksen toiminnan laatua. Järjestelmällisen tietoturvan kehittämisen myötä yritys kykenee myös paremmin arvioimaan tietoturvallisuuden kehittämiseen ja ylläpitoon tarvittavien resurssien määrän.

LÄHTEET

Drucker, P.F. 1970. Muuttumisen aika. Tammi: Helsinki

Erola, E. & Louto, P. 2000 Riskit voimavaraksi - liiketoimintariskien hallinta yrityksessä. Tekijät ja Oy Edita Ab Helsinki

Hakala, M., Vainio, M. & Vuorinen, O. 2006 Tietoturvallisuuden käsikirja Docendo Finland Oy Jyväskylä

Järvinen, P. 2002 Tietoturva & yksityisyys. Docendo Finland:Porvoo

Kajava, J. & Siponen, M. 2002 Security Management and Organizations - Bottom up or Top down Approach? European Intensive Programme on Information and Communication Technologies Security, IPICS'2002, 3rd Winter School.

Karvonen, E. 2000. Elämmekö tietoyhteiskunnassa vaiko informaatioyhteiskunnassa? Tiedon ja informaation käsitteiden syväanalyysiä. Teoksessa: Vuorensyrjä ja Savolainen (toim.) Tieto ja tietoyhteiskunta. Gaudeamus: Helsinki

Knuuttila, E. 1997 Tietoriskien tarkastuksen ja riskienhallinnan käsikirja. Suomen ATK-kustannus Oy Jyväskylä

Kurtz, R. Vines, R. 2003 Tietoturvasertifikaatti - CISSP, Edita Prima Oy Helsinki

Kuusela, H. & Ollikainen, K. 2005 Riskit ja riskienhallinta Tampereen yliopistopaino Oy - Juvenes Print Tampere

Leppänen, J. 2006 Yritysturvallisuus Käytännössä, Turvallisuusjohtamisen portfolio. Talentum Helsinki.

Miettinen, J. 1999 Tietoturvallisuuden johtaminen -näin suojaat yrityksesi toiminnan. Gummerus kirjapaino Oy Helsinki

Miettinen, J. & Kajava, J. 1994 Tietoriskien arviointi Risk Analysis and Risk Assesment - An Overview of Ideas and Techniques

PK-RH. 2000 – 2009. Pk-yrityksen riskienhallinta
Viitattu 15.11.2010 http://www.pk-rh.com/

Riski analyysit. Potentiaalisten ongelmien analyysi. VTT
Viitattu 09.10.2010
http://virtual.vtt.fi/virtual/riskianalyysit/indexef2c.html

Webropol
Viitattu 09.11.2010 http://w3.webropol.com/finland

Tarkistuslistat

INFORMATION SECURITY RISK ANALYSIS SURVEY

INFORMATION SECURITY RISKI MANAGEMENT

Management's Information security risk awareness

1. Business critical information is identified in organization
2. Managers are aware of Business critical information.
3. Information is managed according to local information privacy laws in the organization.

Identifying information risks

1. Situations (such as fire, stealing, accidentally trashing etc.) that might alter or destroy information are identified and known.

Information security risk procedures

1. There is an assigned person responsible for developing information security procedures.

INFORMATION SECURITY OF ENVIRONMENT, WORK AND CUSTOMER FACILITIES

Security of the company building

1. There is access control in the company building.
2. The company building is guarded.
3. Access to common spaces of the company building, such as the phone center, yard, cellar and building roof, is controlled or prevented.
4. There is a crime reporting system in the company building.
5. Windows and outdoors of company building are always locked when there are no authorised people inside.

Security of company facilities (our facilities within the company building)

1. There is an assigned person responsible for managing access rights to company facilities.
2. Unauthorised traffic inside company facilities is limited and controlled – e.g. personal office room doors are locked.
3. External persons who have keys to company facilities are identified and carefully controlled – e.g. cleaner, janitor.
4. Working in company facilities after office hours is controlled (e.g. working times, access control supervisors are aware when and why their employees are in the office).
5. There is an appropriate visitor procedure and everyone are aware of it.
6. Important devices such as workstations and servers are located in controlled spaces.
7. Server space security is appropriate for business operation.
8. Server space is protected against power blackouts.
9. All electronic devices are located above floor level (not on floor).
10. There is air-conditioning in the server space.
11. There is fire alarm and reporting system in the server space.
12. Employees have practice using fire extinguishing equipment.
13. Evacuation of company facilities and building is practiced in case of emergency situations such as fire.

Visits by potential customers, customers and partners

1. There is no confidential information in visitor spaces (such as the meeting room).
2. Visitors are not walking by monitors, printers and faxes when entering meeting rooms or customer spaces.
3. Customer spaces are located so that customers can be controlled.
4. Meeting rooms are soundproofed and it is not possible to see inside any meeting room from the outside.
5. Meeting rooms are cleaned after meetings to ensure no information is left in the room – white boards are cleaned, documents or any other information are removed.
6. Devices for visitors are located in spaces where no information security risks exist (e.g. not in somebody's working room).
7. Staff is instructed how they should react to visitors and outsiders
8. During customer and partner visits, we create and sustain an image of trustworthy company that manages information confidentially.
9. Confidential information about the company and its partners and customers is protected (not left/stored in meeting rooms or customer spaces).
10. Background information on new visitors is carefully inspected (foreign and domestic visitors).

PROTECTION OF INFORMATION SYSTEMS

Principles for the use of information systems

1. Information documents are formally classified according to confidentiality.
2. Information is protected and not accessible to unauthorised users.
3. There is an assigned person who manages access rights for information systems.
4. The procedure of access rights admission is documented and everybody knows how it works.
5. The employer's right to read emails of employees in exceptional situations is agreed with employees.
6. Everyone has their own personal username and password to information systems.
7. Employees' access to information resources is limited to information that is relevant to their work tasks.
8. There are locked cabinets for confidential documents and devices.
9. There are shredders and locked waste paper bins for disposing of confidential documents.
10. Use of remote storage (USB-sticks, remote hard disks, CD's) is managed according to procedures and protected by encryption.
11. Information about devices and software is stored in inventory (for maintaining devices and insurance records).
12. There are guidelines for secure remote work practices.
13. There is user authentication for accessing internal company information.
14. Office software packages and programmes used within the company are compatible with each other.
15. Business critical documents are protected by encryption.
16. Data in mobile information devices (e.g. laptops) is encrypted.

INFORMATION SECURITY RISKS AND PRACTICES OF EMPLOYEES

Employees' information security risk awareness

1. Employees know the company's responsibility for information confidentiality and security.
2. Everybody knows what kind of information is confidential and needs to be protected.
3. Everybody knows what kind of information on business operations can be passed on to outsiders. It is everyday practice to classify information documents according to their confidentiality.
4. Employees know where to report information security falses or any weaknesses in information security procedures.
5. It is taken care of that everybody has read and understood documented information management procedures.
6. It is taken care of that everybody has read and understood company information policy.

New Employees

1. It is taken care of when recruiting new employees that they are capable to use company's information systems.
2. It is taken care of when recruiting new employees that they are able to use English language user Interfaces.
3. Information that new employees provide about themselves is checked before the start of their employment relationship.
4. There is a clear procedure for obtaining access rights for new employees, and it is followed in every department.
5. Supervisors are aware about all access rights for new employees.
6. The meaning of confidential agreement and information policy is explained to temporary and new employees.
7. Employees sign an agreement committing them to return all information documents and devices at the end of their employment relationship.

8. New employees are forced to change the default password for their user accounts on information systems.

End of employment relationships between the company and employees

1. There are procedures for ensuring information security at the end of employment relationships.
2. Supervisors are aware of all access rights that should be deleted from systems at end of employment relationships.
3. Supervisors are aware of all work devices, remote storages and documents of resigning employees and takes care that everything is returned to company.
4. There is a procedure for dealing with a fired or resigning employee in conflict situations.
5. If there is a crucial disagreement/lack of trust between employer and employee it is ensured that terminating the employment relationship is legal and possible to justify by formal documents.
6. There is a contingency plan to deal with employees' main tasks – business operation is not suspended in case of instant resignation or longer absence of an employee.

Use of information systems and workstations

1. It is taken care of that employees have sufficient basic knowhow in the use of information systems, devices and software.
2. Employees are supported in case of interruption in function or malfunction of devices and information systems.
3. Every employee uses only his or her own user accounts for information systems.
4. Care is taken to ensure that employees use secure passwords.
5. Every employee is guided to lock his or her workstation when unattended.
6. Unauthorised persons cannot read, delete or modify employees' personal data in workstation or information systems.
7. There are guidelines for making backups (workstations, servers) and retrieving information from backups.
8. Making backups of personal workstation is centrally controlled.
9. There is an information policy for internet use and employees are aware of it.
10. There is an information policy for email use and employees are aware of it.
11. Workstations are virus protected and employees are aware of it.
12. Employees are forbidden to install any personal software on work devices or company network.